TLfDI

Thüringer Landesbeauftragter
für den **Datenschutz** und die **Informationsfreiheit**

11. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

Vorbemerkungen zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361/3771900, Telefax: 0361/3771904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: Druckhaus Gera GmbH
Jacob-A-Morand-Straße 16, 07552 Gera
Telefon: 0365/737520
E-Mail: info@druckhaus-gera.de

Redaktionsschluss: 17.05.2016

Bildnachweis: TLfDI

11. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2014 bis 31. Dezember 2015
Zitiervorschlag: 11. TB LfDI Thüringen

Der 11. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Mai 2016

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Anlagen

Entschließungen der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg

Entschließungen zwischen den Konferenzen 2014

Entschließungen der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg

Pressemitteilung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg

Entschließungen zwischen den Konferenzen 2014/2015

Entschließungen der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Gemeinsame Pressemitteilung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Entschließungen zwischen den Konferenzen 2015

Entschließungen der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30. September/1. Oktober 2015 in Darmstadt

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 15./16. September 2015)

Pressemitteilungen 2014

Pressemitteilungen 2015

Veranstaltungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit 2014

Veranstaltungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit 2015

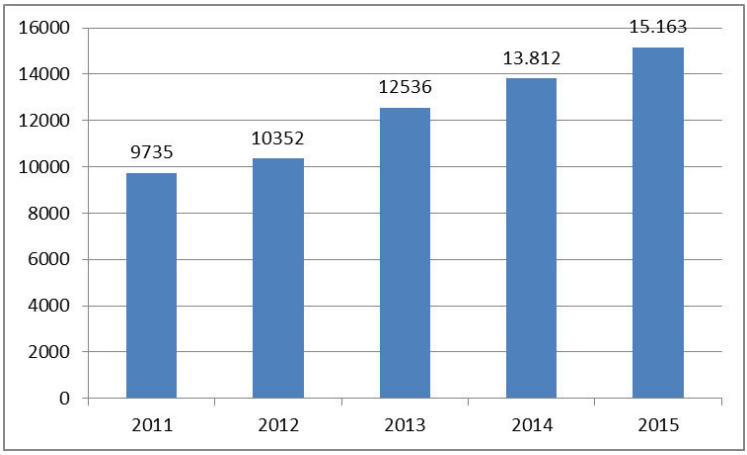
A Öffentlicher Bereich

Vorwort

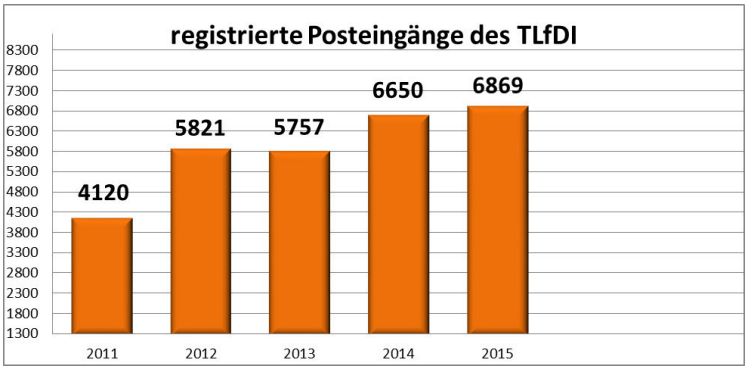
Dr. Lutz Hasse

Der Umfang des 11. Tätigkeitsberichts zeigt, dass der Arbeitsanfall beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter angewachsen ist. Der Tätigkeitsbericht wird immer dicker! Die immense Zahl der Beiträge machte es sogar notwendig, dass der 11. Tätigkeitsbericht für den öffentlichen Bereich und der 2. Tätigkeitsbericht für den nicht-

öffentlichen Bereich in zwei gesonderten Bänden veröffentlicht werden.
Vorab sei angemerkt, dass sich die Beiträge nahezu ausschließlich auf den Berichtszeitraum beziehen. Wenn es nach dem Ende des Berichtszeitraums eine wesentliche Änderung gegeben hat, gibt es einen entsprechenden Hinweis.
Insgesamt wurden beim TLfDI im Berichtszeitraum 28.975 Dokumente im Dokumentenmanagementsystem erstellt (13.812 im Jahr 2014 und 15.163 im Jahr 2015). Vergleicht man diese Zahlen mit denjenigen der letzten Jahre seit Einführung des Dokumentenmanagementsystems, ist ein kontinuierlicher Anstieg zu verzeichnen.



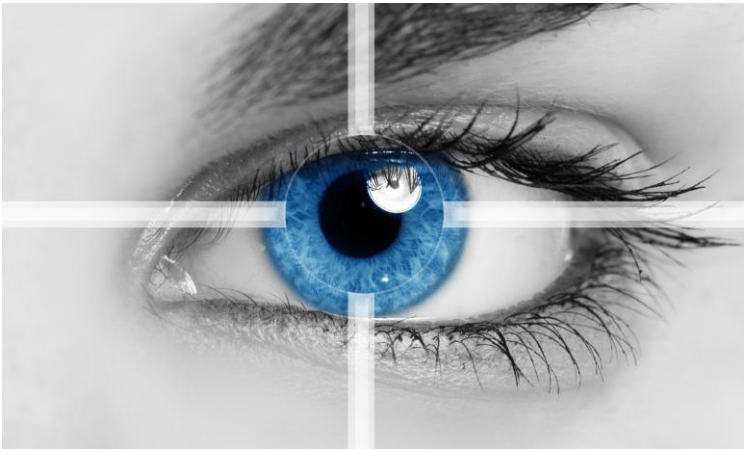
Diese Zahlen erfassen alle beim TLfDI elektronisch angelegten Dokumente, also Posteingänge und Postausgänge sowie interne Vermerke.
Sieht man sich lediglich die Posteingänge an, ergibt sich ein ähnliches Bild:



Auch in den Jahren 2014/2015 ist daher die personelle Situation der Behörde nach wie vor äußerst angespannt. Aufgrund der wachsenden Zahl der Eingaben und auch wegen der zunehmenden Komplexität datenschutzrechtlicher Fragestellungen kommt die Behörde immer wieder an ihre Grenzen. Anlassunabhängige Kontrollen sind daher nur noch in begrenztem Umfange möglich und die Bearbeitung von Anfragen und Beschwerden kann leider nicht immer zeitnah erfolgen. Trotzdem ist festzustellen, dass die Mitarbeiter der Behörde hochmotiviert alle Beschwerden, egal, ob sie namentlich oder anonym erhoben werden, bearbeiten und allen Hinweisen nachgehen. Daher möchte ich mich an dieser Stelle ausdrücklich bei meinen Mitarbeitern bedanken, die sehr oft „am Anschlag“ arbeiten und ohne deren unermüdlichen Einsatz es um den Datenschutz in Thüringen wesentlich schlechter bestellt wäre. Die Arbeit wird dabei nie zur Routine, weil die technische Entwicklung immer neue Datenschutzfragen aufwirft. Hinzu kommt, dass mit dem baldigen Inkrafttreten der Datenschutzgrundverordnung der Europäischen Union neue Herausforderungen auf den TLfDI zukommen. Da die Datenschutzgrundverordnung unmittelbar gelten wird, ist ein Großteil des bislang zur Anwendung kommenden Rechts Makulatur. Die öffentlichen Stellen müssen die Anforderungen der neuen Regelungen umsetzen und der TLfDI wird sie hierbei tatkräftig unterstützen. Daher muss die ganze Behörde sich bereits vorher mit den neuen Regelungen vertraut machen. Ich habe dem dafür zuständigen Ressort bereits Unterstützung bei der Schaffung von neuen Landesregelungen angeboten. Deutlich zeichnet sich ab: Die Arbeit wird nicht weniger, sondern schnell mehr. Soll die Leistungsfähigkeit der Behörde lang-

fristig erhalten bleiben, bedarf es dringend einer Aufstockung des Personals. Auf die weitere Förderung durch die Landtagsfraktionen muss und darf der TLfDI vertrauen.

Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: https://www.tlfdi.de/tlfdi/). Dadurch kann auf Geräten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden Software der Link durch das Gerät wieder decodiert werden und „Abschreibfehler“ können vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers „Marty Mouse“ in der Version 1.0 empfohlen werden, da hier Open-Source-Software genutzt wird und die App nur minimale Funktionen besitzt. Für iOS ist dem TLfDI keine datenschutzgerechte App bekannt.



Eye close-up – © Minerva Studio / Fotolia.com

1 Schwerpunkte im Berichtszeitraum

Ein maßgeblicher Schwerpunkt der Arbeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war die Entwicklung des Datenschutzrechts auf europäischer Ebene. Die Datenschutzgrundverordnung der Europäischen Union soll die für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen geltenden Regelungen europaweit vereinheitlichen. Da aber viele Mitgliedstaaten der Europäischen Union kein so wirksames Datenschutzrecht haben wie Deutschland, galt es zu verhindern, dass das Datenschutzniveau in Europa weit hinter dem in Deutschland geltenden Standard abfällt. Der TLfDI wirkte an Positionspapieren und Entschließungen der Datenschutzkonferenz zur Datenschutzgrundverordnung mit. Wichtig war dabei, besonders zu definieren, welche Mindeststandards künftig gelten sollen (siehe dazu Nr. 3.2.). Im Schatten der Datenschutzgrundverordnung wurde auch die EU-Richtlinie für Justiz und Inneres (JI-Richtlinie) verhandelt, durch die der Datenschutz für die Erhebung, Speicherung, Weitergabe und Verarbeitung für Polizei, Justiz und Inneres europaweit vereinheitlicht werden soll (siehe dazu Nr. 3.3.).

Zu nennen ist auch die Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015. Seit dem Tag der Entscheidung wechselten sich Abstimmungen, E-Mails über neueste Entwicklungen und Termine sowie Sondersitzungen der Datenschutzkonferenz im Tagesrhythmus ab. Zu klären war, welche Rechtsgrundlagen Behörden nach dem EuGH-Urteil, das die Safe-Harbor-Entscheidung für nichtig erklärt hatte, alternativ für Datenübermittlungen in die USA nutzen konnten (siehe dazu im Einzelnen Nr. 3.1 sowie Anlage 22).
Seit Ende Februar 2016 ist nunmehr mit "Privacy Shield" das geplante Nachfolgeabkommen zu "Safe Harbor" bekannt. Die Art. 29-Datenschutzgruppe der Europäischen Datenschutzbeauftragten hält aber auch die Privacy-Shield-Regelungen an mehreren Stellen für mit dem europäischen Datenschutzstandard nicht vereinbar.
Der Datenschutz in den Thüringer Kommunen war ebenfalls ein großer Aufgabenschwerpunkt im Berichtszeitraum: Als Klassiker in der Aufgabenstellung für den TLfDI sind hier die Übertragung von Sitzungen des Stadtrates im Internet sowie die Videoüberwachung durch Städte und Gemeinden zu nennen. Aber auch Kuriositäten fanden sich in der Aufgabenliste des TLfDI: Von unrechtmäßig erhobenen personenbezogenen Daten aus einer Unterschriftensammlung, über Anrufe angeblicher Interessenten (mystery calls) bei Hotels und Pensionen im Thüringer Wald bis hin zum Fund einer ausgemusterten Festplatte mit personenbezogenen Daten aus einem kommunalen Betrieb auf einer Müllkippe war alles dabei.
Sehr viele Fälle gab es auch im Bereich des Beschäftigtendatenschutzes. Die fortschreitende Technologisierung der Arbeitswelt ermöglicht es den Dienstherren, auf immer leichterem Weg Mitarbeiter zu überwachen. Im medizinischen Bereich ist die Tendenz zu verzeichnen, dass die verschiedenen Akteure sich zum Informationsaustausch immer stärker vernetzen. Dies betrifft den Bereich der Forschung aber auch die konkrete Behandlung eines Patienten. Hier gilt es, streng darauf zu achten, dass die Datenübertragung sicher ist und die Zugriffsrechte sich an der Erforderlichkeit der Aufgabenerfüllung orientieren.
Die Informationstechnik (IT) hat nun endgültig nicht nur im privaten Sektor, sondern auch im öffentlichen Sektor Einzug gehalten. Kaum ein Lebensbereich ist heutzutage noch ohne IT denkbar. Innerhalb der Cyberkriminalität werden zunehmend zwei Trends sichtbar. Seit Jahren versuchen Hacker private Rechner zu kapern, um Daten auf den Rechnern auszuspionieren, die elektronische Kommunikation

mitzulesen oder zu manipulieren oder die Rechner für einen gemeinsamen programmierten Angriff zu nutzen (Bot-Netze). Hilfe für die Bürger seitens des Staates gab es bis dato kaum. Erst mit den Hackerangriffen auf Behördenstrukturen und Wirtschaftsunternehmen erfolgte ein Umdenken der Politik und man kreierte die „Cyber-Sicherheitsstrategie“. Dem folgte ein IT-Sicherheitsgesetz, welches nun die Erhöhung der Sicherheit in informationstechnischen Systemen regelt. So wurden als kritische Infrastrukturen, und damit als besonders schutzwürdig, Sektoren der Energie, der Informationstechnik und Telekommunikation, des Transportes und des Verkehrs, der Gesundheit, des Wasser, der Ernährung sowie des Finanz- und Versicherungswesens definiert (siehe dazu Nr. 15.7.). Mit dem Ergebnis, dass Diensteanbieter nunmehr die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden dürfen, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Der Schutz für die Bürger und ihre Daten selbst bleibt dabei aber weiterhin auf der Strecke. So fordern die Datenschutzbeauftragten des Bundes und der Länder seit Jahren eine sichere IT-Infrastruktur für die Bürger und eine sichere Ende-zu-Ende-Verschlüsselung (siehe dazu die Nummern 15.1 und 15.5). Es bleibt bspw. nicht nachvollziehbar, dass gemäß § 27 Abs. 3 Personalausweisgesetz der Personalausweisinhaber durch technische und organisatorische Maßnahmen gewährleisten muss, dass der elektronische Identitätsnachweis nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Der Bürger also selbst einen hohen Stand an IT-Sicherheit gewährleisten muss, wissend, dass dies nicht mal der Staat für sich selber sicherstellen kann. Wo der Staat sich nicht selber schützen kann, soll es der Bürger. Hier bedarf es dringend eines Umdenkens der Politik. Zukünftig müssen mindestens die Verfahren, die auf Länder- oder Bundesebene den Bürgern angeboten werden auch einheitlich und datenschutzgerecht gestaltet werden. Dies bedeutet, wenigstens sichere Verschlüsselungsverfahren anzubieten, die eine echte Ende-zu-Ende-Verschlüsselung ermöglichen, die nicht vom Staat und von Unbefugten eingesehen werden kann. Zudem bedarf es dringend einer für den normalen Bürger handhabbaren und finanzierbaren qualifizierten elektronischen Signatur-Möglichkeit, um rechtssicher Dokumente auszutauschen. Dabei ist die Politik in Deutschland gut beraten, wenn sie es zeitnah selbst umsetzt, denn zukünftig wird man sich europaweit eine qualifizierte elektronische

Signatur kaufen können. Der Preis – nicht die Sicherheit – wird auschlaggebend werden, ob in Deutschland in nächster Zeit qualifizierte elektronische Signaturen im großen Umfang einsetzbar sind oder nicht.

Datenschutz – © fotodo / Fotolia.com

2 Allgemeine Entwicklungen im Datenschutz

2.1 Überblick

Das Grundrecht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsurteil vom 12. Dezember 1983 aus den Artikeln 2 Abs. 1 und 1 Abs. 1 Grundgesetz entwickelte, hat nichts an Aktualität eingebüßt. Das Grundrecht besagt im Kern, dass jeder grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können muss.

Neben den großen aktuellen „Baustellen“ des Datenschutzrechts, nämlich der Europäischen Datenschutzgrundverordnung (DSGVO) (vgl. Beitrag Nummer 3.2), der Datenschutzrichtlinie im Bereich Inneres und Justiz (JI-Richtlinie) (siehe Beitrag Nummer 3.3) und der Frage, welche Alternativen es zur nichtigen Safe-Harbor-Entscheidung der Kommission für eine Datenübermittlung in die Vereinigten Staaten von Amerika gibt (siehe hierzu Beitrag Nummer 3.1), sind auch noch folgende Ereignisse und Ge-

richtsentscheidungen für den Datenschutz von besonderer Bedeutung gewesen:
Der Deutsche Bundestag hatte am 20. März 2014 auf Antrag aller Fraktionen die Einsetzung eines Untersuchungsausschusses beschlossen (BT Drucks. 18/843), der die Hintergründe und das Ausmaß ausländischer nachrichtendienstlicher Ausspähungen aufklären soll (NSA-Untersuchungsausschuss). Dieser war im Berichtszeitraum noch nicht abgeschlossen, sodass über den Abschluss und die Ergebnisse wohl erst im kommenden Tätigkeitsbericht berichtet werden kann. Der TLfDI hatte bereits in seinem 10. Tätigkeitsbericht (siehe 10. Tätigkeitsbericht, Nummer 2.2 Snowden, NSA, PRISM, Tempora und Antiterrordatei – das Jahr 2013 als „datenschutzrechtlicher Durchlauferhitzer“, Seite 26) darauf hingewiesen, dass die Bundesregierung gefordert bleibe, auf politische Lösungen hinzuwirken. Vielleicht bewirken die Empfehlungen des NSA-Untersuchungsausschusses, die es mit Sicherheit nach Beendigung seiner Arbeit geben wird, einen verbesserten Schutz von personenbezogenen Daten gegenüber deutschen und anderen Geheimdiensten.
Neben dem wegweisenden Urteil des Europäischen Gerichtshofes (EuGH) zu Safe Harbor dürfen an dieser Stelle auch zwei weitere wichtige Urteile nicht unerwähnt bleiben:
Mit seinem Urteil vom 8. April 2014 (Az.: C-293/12 und C-594/12 [verbundene Rechtssachen]) erklärte der EuGH die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, für ungültig. Der EuGH stellte in seiner Entscheidung fest, dass die Verpflichtung zur Vorratsdatenspeicherung und der Zugriff der zuständigen nationalen Behörden auf diese Daten ein besonders schwerwiegender Eingriff der Richtlinie in die Grundrechte auf die Achtung des Privatlebens und auf Schutz personenbezogener Daten ist. Aus der Gesamtheit der Daten könnten genaue Rückschlüsse auf die Gewohnheiten von Personen, ihre Aufenthaltsorte, ihre ausgeübten Tätigkeiten und auch auf das soziale Umfeld gezogen werden. Der EuGH urteilte, dass der europäische Gesetzgeber beim Erlass der Richtlinie die Grenze der Verhältnismäßigkeit überschritten habe. Die Datenschutzbeauftragten des Bundes und der Länder begrüßten diese Entscheidung des EuGH und wiesen in ihrer Entschließung „Keine Vorratsdatenspeicherung in Europa!“ vom 25. April 2014 (siehe hierzu Anlage 8) darüber hinaus ausdrücklich

darauf hin, dass der Maßstab des EuGH auch für das anlasslose, exzessive Überwachen durch sämtliche Nachrichtendienste gelten müsse.
Nichtsdestotrotz trat am 18. Dezember 2015 in Deutschland das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten in Kraft (Drucksache 18/5088). Quasi „durch die Hintertür“ wurde damit zugleich der neue Straftatbestand der Datenhehlerei eingeführt, § 202d Strafgesetzbuch. Diesem Straftatbestand wird zur Last gelegt, dass er unpräzise formuliert sei und daher eine kritische Berichtrecherche durch Journalisten zumindest behindern kann. Es bleibt daher spannend abzuwarten, ob auch diese Regelungen wieder einmal vom Bundesverfassungsgericht aufgehoben werden.
Mit seiner Entscheidung vom 13. Mai 2014 (Az.: C-131/12 „Google Spain“) urteilte der EuGH, dass ein Suchmaschinenbetreiber (hier: Google Spain) unter bestimmten Voraussetzungen verpflichtet ist, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über eine Person von seiner Ergebnisliste entfernen muss. Der EuGH schuf mit diesem Urteil das „Recht auf Vergessenwerden“, das auch die neue Europäische Datenschutzgrundverordnung (DSGVO) erstmals in Art. 17 regelt. Betroffene Personen können sich nach dem EuGH-Urteil nunmehr direkt an die jeweiligen Suchmaschinenbetreiber wenden und von ihnen verlangen, dass bei der Suche einzelne Links zu ihrem Namen nicht mehr angezeigt werden. Unangetastet lässt das Urteil die Löschung der Inhalte selbst, diese bleiben weiterhin frei zugänglich. Der EuGH entschied, dass der Suchmaschinenbetreiber selbst Daten verarbeite und somit als verantwortliche Daten verarbeitende Stelle zu qualifizieren sei. Da es sich bei Google Spain um eine Tochtergesellschaft von Google Inc. in Spanien handele, sei diese als Niederlassung im Sinne der Europäischen Datenschutzrichtlinie 95/46/EG anzusehen.
Die Datenschutzbeauftragten des Bundes und der Länder sahen in dem Urteil einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Oktober 2014; „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ (siehe dazu Anlage 12). Das Urteil muss nun von den einzelnen Suchmaschinenbetreibern umgesetzt werden.

Mit Sorge betrachtet der TLfDI die Auswertung von Big Data durch Unternehmen und Behörden. Datenfluten aus Smart /Cars/Meters/Houses/Cities etc., Gesundheitsdaten aus Wearables, das Scannen der Umwelt mit Smart-Glasses, Dash-Cams, die Masse von ungetesteten Apps mit unbekannten Funktionen und dann noch das Filtern und Auswerten dieser Datenfluten mithilfe von Algorithmen, um etwa Profile über jedermann und jedefrau zu erstellen, die allem Möglichen dienen, nicht nur Werbezwecken. Das Grundrecht auf informationelle Selbstbestimmung ist bedroht, und insbesondere der Gesetzgeber sollte es schützen wollen. Allerdings sind die Normen hierfür von vorgestern. Warum werden die Datenschutzbeauftragten nicht stärker in die Regelungsprozesse eingebunden? Weil sie die Bedenkenträger sind, die niemand hören will? – Ein Luxus, den man sich nicht mehr lange wird leisten können, wenn man es mit dem Schutz der Privatsphäre als Teil der Menschenwürde ernst meint. Zudem muss der Schutz der Privatsphäre bereits in der Schule oder noch früher vermittelt werden können. Hierzu sind die Lehrer mittels Aus- und Fortbildungsveranstaltungen in die Lage zu versetzen. Als Vorsitzendem des Arbeitskreises Datenschutz und Bildung ist es dem TLfDI gelungen, die Datenschutzbeauftragten der Länder und Vertreter der Kultusministerkonferenz zusammenzubringen – Datenschutzbeauftragte und Lehrer wollen auf diese Weise erstmals gemeinsam Medienkompetenz einschließlich Privatsphärenschutz den Lehrern, Schülern, aber auch den Eltern näherbringen. Ein lohnendes Unterfangen, das auch die Unterstützung des Thüringer Kultusministeriums genießt.

Wenn der Gesetzgeber das Recht auf informationelle Selbstbestimmung gemäß Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG oder insbesondere die Grundrechte aus Art. 7 und Artikel 8 der Charta der Grundrechte der Europäischen Union nicht hinreichend in Gesetzen beachtet, ist auf das Bundesverfassungsgericht und den Europäischen Gerichtshof als Korrektiv Verlass: Vorratsdatenspeicherung, Google-Spain oder Safe Harbor sind nur drei Schlagworte aus dem Berichtszeitraum, die belegen, wie wichtig es ist, dass eine unabhängige Justiz funktioniert. Dafür lohnt es sich, zu streiten. Der Gesetzgeber darf modernen Entwicklungen nicht mit antiquierten Datenschutzregelungen hinterherhinken.

2.2 Wann dürfen öffentliche Stellen einen externen Datenschutzbeauftragten haben?

Immer wieder wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit sowohl von öffentlichen Stellen als auch von externen Datenschutzbeauftragten gefragt, ob eine Bestellung eines externen Datenschutzbeauftragten möglich ist, ohne dass dieser Beschäftigter der öffentlichen Stelle ist. Diese Frage beantwortet das Gesetz klar. Nach § 10a Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) haben Daten verarbeitende Stellen, die personenbezogene Daten mithilfe automatisierter Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Aus dieser Formulierung geht hervor, dass der Beauftragte für den Datenschutz Beschäftigter der jeweiligen öffentlichen Stelle sein muss. Eine Ausnahme besteht nach § 10a Abs. 6 ThürDSG für die staatlichen Schulen. Hier kann die Aufsichtsbehörde einen ihrer Beschäftigten zum Beauftragten für den Datenschutz bestellen.
Etwas anderes gilt für juristische Personen oder sonstige Vereinigungen, die nach § 2 Abs. 2 ThürDSG als öffentliche Stellen gelten, wenn sie am Wettbewerb teilnehmen. In diesem Fall sind nach § 26 ThürDSG auf sie die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mit Ausnahme des zweiten Abschnitts des § 38 anwendbar. Dies betrifft beispielsweise öffentliche Schwimmbäder oder Krankenhäuser. Die einschlägige Regelung des § 4f BDSG enthält eine derartige Beschränkung auf eigene Beschäftigte nicht.

Einen externen Datenschutzbeauftragten, der nicht Beschäftigter der verantwortlichen Stelle ist, dürfen öffentliche Stellen nur dann haben, wenn sie nach § 26 ThürDSG dem BDSG unterfallen, weil sie am Wettbewerb teilnehmen.

2.3 Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes (BMG)

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm im Berichtszeitraum zum Referentenentwurf eines Thüringer Gesetzes zur Ausführung des Bundesmeldegesetzes (ThürAGBMG) und zur Änderung weiterer Gesetze Stellung.

Darüber hinaus äußerte sich der TLfDI im Rahmen des Anhörungsverfahrens gemäß § 112 Abs. 4 Geschäftsordnung des Thüringer Landtags gegenüber dem zuständigen Ausschuss zum o. g. Thema.
Seit dem 23. September 2015 ist das Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes in Kraft (GVBl. S. 131).
Im Ergebnis wurden die aus datenschutzrechtlicher Sicht erforderlichen Änderungswünsche des TLfDI zum Teil umgesetzt. So wurde der Forderung entsprochen, bei der Datenübermittlung zwischen den Meldebehörden das Übertragungsprotokoll OSCI-Transport und bei der Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften auch das Übertragungsprotokoll OSCI-Transport einzusetzen, wenn die öffentlich-rechtlichen Religionsgesellschaften dem zugestimmt haben. Somit werden die Daten mittels einer Ende-zu-Ende-Verschlüsselung sicher übertragen, sodass kein Unbefugter Kenntnis erlangen kann.
Leider wurden die bestehenden datenschutzrechtlichen Bedenken und Ergänzungswünsche bezüglich § 2 Abs. 1 Nr. 2 ThürAGBMG nicht aufgenommen.
Eine verbindliche Regelung zur Löschung dieser Daten wird weiterhin für dringend erforderlich erachtet. Wenn es bspw. in einem Wahl- bzw. Abstimmungsbezirk nur eine Unterstützerliste gab, kann später immer noch genau recherchiert werden, welcher Bürger eine Unterstützungsunterschrift leistete. Selbst bei zwei Unterstützerlisten kann gerade im ländlichen Gebiet später u. U. noch eine Zuordnung möglich sein.
Mit Wirkung vom 1 November 2015 ist die Thüringer Meldeverordnung (GVBl. 2016, 49) in Kraft getreten, an der der TLfDI seitens des Thüringer Ministeriums für Inneres und Kommunales (TMIK) ebenfalls beteiligt wurde und über die er im Einzelnen im nächsten Tätigkeitsbericht informieren wird.

Der TLfDI hält eine verbindliche Regelung zur Löschung der erfassten Daten bei Unterstützerlisten bei Wahlen weiterhin für erforderlich. Der TLfDI wird ein „datenschutzrechtliches Auge“ auf die Ausführung des Bundesmeldegesetzes in Thüringen haben müssen.

2.4 Datenerfassung beim Waffenregister – verkantet?

Über die Einrichtung des Nationalen Waffenregisters beim Bundesverwaltungsamt informierte der Thüringer Landesbeauftragte für den

Datenschutz und die Informationsfreiheit (TLfDI) im 10. Tätigkeitsbericht unter Punkt 2.9. Zudem berichtete der TLfDI über eine Kontrolle in einer Waffenbehörde, bei der Mängel zutage traten.
Infolgedessen kontrollierte der TLfDI 2015 erneut diese sowie eine weitere Waffenbehörde, um den Umgang mit personenbezogenen Daten zu überprüfen. Wie bereits 2013 festgestellt, waren in der betreffenden Waffenbehörde die Unterlagen in Regalen und nicht, wie erforderlich, in verschließbaren Schränken untergebracht.
Auch nach einer entsprechenden Beanstandung im März 2014 wurden die notwendigen Vorkehrungen aus haushaltstechnischen Gründen nicht getroffen.
Sowohl bei der Kontrolle 2015 als auch zum Redaktionsschluss des vorliegenden Tätigkeitsberichtes waren die vorhandenen offenen Regale weiterhin nicht durch zusätzliche Türen geschützt oder durch neue Schränke ausgetauscht worden.
Wegen der weiterhin offen zugänglichen Lagerung von Unterlagen ist deshalb nicht auszuschließen, dass außerhalb der Bürozeiten oder in der Urlaubszeit des zuständigen Sachbearbeiters die in den Unterlagen enthaltenen personenbezogenen Daten von unbefugten Dritten zur Kenntnis genommen werden können.
Dies stellt weiterhin einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Die zwischenzeitlich getroffene organisatorische Festlegung, dass keine Unbefugten ohne Anwesenheit einer berechtigten Person Zugang zu den Büros der Waffenbehörde haben dürfen, mildert diesen festgestellten Verstoß aus Sicht des TLfDI nicht ab.
Dem TLfDI wurde auf Nachfrage mitgeteilt, dass im Haushaltsplan 2016 vom zuständigen Fachamt finanzielle Mittel zur Nachrüstung angemeldet wurden. Sofern der Haushaltsplan 2016 vom Kreistag bestätigt und durch die Aufsichtsbehörde genehmigt wird, würde entsprechend nachgerüstet werden.
Weiterhin wurde im Zuge der Kontrollen in den betreffenden Waffenbehörden bei einer stichprobenartigen Prüfung der Eingabemasken bezüglich des lokalen Waffenregisters festgestellt, dass die Eingabefelder „Erlernter Beruf“ und „derzeit ausgeübter Beruf“ vorhanden waren. Der TLfDI musste dabei feststellen, dass bei einer Anzahl von Datensätzen diese Angaben auch ausgefüllt waren. Auch das papiergebundene Formular „Antrag auf Erteilung einer waffenrechtlichen Erlaubnis“ enthält beide Felder „Erlernter Beruf“ und „derzeit ausgeübter Beruf“. Auf Nachfrage zur Notwendigkeit der

Felder erhielt der TLfDI in beiden Waffenbehörden die Antwort, dass man diese Angaben eigentlich nicht benötige. Regelungen, wann diese Felder auszufüllen sind, seien auch nicht vorhanden.
Gemäß § 6 Waffengesetz (WaffG) ist die persönliche Eignung von Personen zum Besitz von Waffen zu beurteilen. Dies kann aus Sicht des TLfDI grundsätzlich aber unabhängig vom Beruf der zu beurteilenden Person erfolgen. Allerdings gesteht der TLfDI dem Datum „derzeit ausgeübter Beruf“ immerhin eine Indizwirkung zu, wenn besondere Erlaubnistatbestände für bestimmte Personengruppen eine Rolle beim Erteilen der Waffenerlaubnis zu berücksichtigen sind. So kann gemäß WaffG bei Jägern (§ 13), Sachverständigen (§ 18), gefährdeten Personen (§ 19), Waffenherstellern und Waffenhändlern (§§ 21, 26), Bewachungsunternehmern und Bewachungspersonal (§§ 28, 28a) der Beruf tatsächlich als allgemeines Kriterium zur Beurteilung der persönliche Eignung von Personen zum Besitz von Waffen Verwendung finden.
Eine Erfassung des erlernten und des derzeitig ausgeübten Berufes bei allen Antragstellern sieht der TLfDI allerdings nicht für erforderlich an. Deshalb bat er die betroffenen Waffenbehörden um Stellungnahmen bis Ende März 2016, um ggf. landes- oder bundesweit eine einheitliche Lösung anzustreben. Diese sind zwischenzeitlich eingetroffen und werden im kommenden Berichtszeitraum geprüft.

Akten und Unterlagen mit personenbezogenen Daten in Waffenbehörden müssen vor dem Zugang unbefugter Dritter geschützt werden. Die notwendige Erfassung der Daten „erlernter Beruf“ und „derzeit ausgeübter Beruf“ für alle Antragsteller wird derzeit vom TLfDI geprüft.

2.5 Wissensdurstige Meldebehörde – nach dem neuen Bundesmeldegesetz Durst zulässig

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Hausverwalters, der sich erkundigte, ob folgendes Auskunftsersuchen der Meldebehörde zulässig sei: Als ein durch den Wohnungsgeber beauftragter Hausverwalter habe er Daten eines Mieters der Meldebehörde mitteilen müssen.
Als Wohnungsgeber gemäß § 17 des neuen Bundesmeldegesetzes (BMG) kommt grundsätzlich der Wohnungseigentümer, mit dem ein

Mietvertrag geschlossen wird, in Betracht. Es kann sich aber auch um den Hauptmieter handeln, mit dem ein Untermietverhältnis besteht.
Grundsätzlich bestehen verschiedene Mitwirkungsverpflichtungen des Wohnungsgebers oder einer von ihm beauftragten Person im Zusammenhang mit Meldeangelegenheiten nach dem BMG.
Zunächst hat der Wohnungsgeber nach dem BMG den Einzug oder den Auszug der meldepflichtigen Person, also dem Mieter, schriftlich oder elektronisch innerhalb der in § 17 Absatz 1 oder 2 BMG genannten Fristen zu bestätigen (§ 19 Abs. S. 2 BMG). Diese Verpflichtung besteht seit dem 1. November 2015, dem Inkrafttreten des neuen BMG.
Die Auskunftspflicht des Wohnungsgebers gegenüber dem Mieter zur Vorlage bei der Meldebehörde nach § 19 Abs. 1 S. 2 BMG umfasst folgende Angaben:

- Name und Wohnanschrift des Wohnungsgebers,
- Art des meldepflichtigen Vorgangs mit Einzugs- oder Auszugsdatum,
- Anschrift der Wohnung sowie
- Namen der nach § 17 Absatz 1 und 2 BMG meldepflichtigen Personen.

Verweigert der Wohnungsgeber diese Bestätigung, hat der Mieter als meldepflichtige Person dies der Meldebehörde unverzüglich mitzuteilen. Versäumt der Wohnungsgeber das Ausstellen der Bestätigung, sieht das Bundesmeldegesetz dafür Bußgelder von bis zu 1.000 Euro vor. Bis zu 50.000 Euro Bußgeld sind möglich, wenn eine Person nur zum Schein in einer Immobilie angemeldet wird.
Daneben beinhaltet die in § 19 BMG geregelte Mitwirkungspflicht auch die Auskunft des Eigentümers und, wenn er nicht selbst Wohnungsgeber ist, auch vom Wohnungsgeber über die Personen, welche bei ihm wohnen oder gewohnt haben. Diese Auskunftsverpflichtung des Eigentümers oder des Wohnungsgebers ergibt sich aus § 19 Abs. 5 BMG.
Der vom Beschwerdeführer dargelegte Sachverhalt ist der Auskunftsverpflichtung des Wohnungsgebers nach § 19 Abs. 5 BMG zuzuordnen, da sich die Meldebehörde unmittelbar an ihn als vom Wohnungsgeber beauftragte Person gewandt hatte. Der Beschwerdeführer hat keine Tatsachen vorgetragen, die darauf schließen lassen konnten, dass das Auskunftsbegehren der Meldebehörde unzulässig

gewesen sei. Deswegen war vom TLfDI in dieser Angelegenheit nichts weiter zu monieren oder zu beanstanden.
Die Mithilfe des Wohnungsgebers bei Meldeangelegenheiten war im Rahmen der Gesetzesberatungen zum neuen BMG seitens des Gesetzgebers gewollt und ist datenschutzrechtlich nicht zu beanstanden. Das Ansinnen der Meldebehörde, diese Daten vom Wohnungsgeber zu erlangen, ist zulässig, da die Verwendung dieser Daten durch die Meldebehörde eine Verarbeitung im Sinne von § 4 Abs.1 Nr. 1 Thüringer Datenschutzgesetz darstellt, die durch ein Gesetz, hier das BMG, angeordnet wird. Der Wohnungsgeber ist nach § 19 BMG unter Bußgeldandrohung (§ 54 BMG) verpflichtet, die oben näher aufgeführten Daten der Meldebehörde zukommen zu lassen. Dies geschieht entweder mittelbar, indem der Wohnungsgeber dem Mieter eine Bescheinigung nach § 19 Abs. 1 BMG ausstellt, oder aufgrund direkter Auskunftserteilung gegenüber der Meldebehörde nach § 19 Abs. 5 BMG.

Das angeordnete Mitwirken des Wohnungsgebers in Meldeangelegenheiten durch die Übermittlung von in § 19 BMG genannten Daten seiner Mieter mittelbar und unmittelbar an die Meldebehörde ist datenschutzrechtlich nicht zu beanstanden. Die Meldepflicht des Wohnungsgebers dient dem zulässigen Ziel, Scheinanmeldungen zu verhindern. Den dadurch möglicherweise entstehenden Generalverdacht, der Wohnungsgeber vermiete nur zum Schein, hat der Gesetzgeber hier „billigend in Kauf“ genommen.

2.6 Endlich eine Orientierungshilfe zur Videoüberwachung

Dieser Beitrag befasst sich mit der Zulässigkeit der Videoüberwachung nach dem Bundesdatenschutzgesetz (BDSG). Grundsätzlich findet dieses Gesetz auf öffentliche Stellen in Thüringen keine Anwendung. Etwas anderes gilt, wenn die öffentlichen Stellen am Wettbewerb teilnehmen, § 26 Thüringer Datenschutzgesetz (ThürDSG). Für diese so genannten Wettbewerbsunternehmen ist das BDSG in großen Teilen anwendbar und für sie gilt mithin das nachfolgend Gesagte. Für alle anderen öffentlichen Stellen richtet sich die Zulässigkeit der Videoüberwachung allein nach § 25a ThürDSG bzw. nach bereichsspezifischen Normen.
Bereits im letzten Berichtszeitraum war bei allen Aufsichtsbehörden im nicht-öffentlichen Bereich zu beobachten, dass die Videoüberwa-

chung einen immer größeren Stellenwert einnimmt. Dies lag sicherlich auch daran, dass Kameras und Videoüberwachungssysteme zu immer günstigeren Preisen angeboten wurden. Größere Unternehmen haben Filialen in mehreren Bundesländern. Besonders sie waren daran interessiert, dass die datenschutzrechtliche Beurteilung der Videoüberwachung von den Aufsichtsbehörden im Bundesgebiet einheitlich vorgenommen wird. Die Datenschutzkonferenz rief daher eine Ad-hoc-AG Videoüberwachung als Unterarbeitsgruppe des Düsseldorfer Kreises ins Leben. Diese Arbeitsgruppe sollte sich mit speziellen Fragen der Videoüberwachung befassen und dafür sorgen, dass unbestimmte Rechtsbegriffe im Bundesgebiet von Aufsichtsbehörden möglichst einheitlich ausgefüllt werden. Schnell war man sich einig, dass es einer Orientierungshilfe bedarf, um das komplexe Feld der Videoüberwachung datenschutzrechtlich möglichst bundeseinheitlich bewerten zu können. Es gibt im Wesentlichen drei Bestimmungen, nach denen sich die datenschutzrechtliche Beurteilung einer Videoüberwachung richtet:
Dies sind § 6b Bundesdatenschutzgesetz (BDSG) für die Videoüberwachung in öffentlich zugänglichen Bereichen, § 28 BDSG für die Videoüberwachung in öffentlich nicht zugänglichen Bereichen und § 32 BDSG für den Fall, dass Mitarbeiter überwacht werden. Alle drei Bestimmungen enthalten einige unbestimmte Rechtsbegriffe, die es auszufüllen galt. In mehreren Sitzungen wurde die OH „Videoüberwachung durch nichtöffentliche Stellen“ erarbeitet und schließlich vom Düsseldorfer Kreis mit Stand vom 19. Februar 2014 beschlossen. Die OH ist auf der Homepage des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) unter https:// tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh-v__-durch-nicht-__ffentliche-stellen.pdf veröffentlicht.

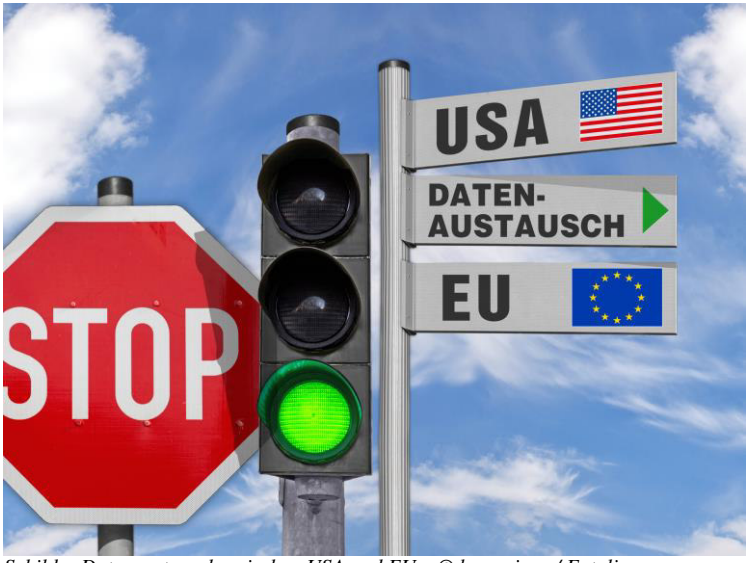
Der TLfDI hat an der Erarbeitung der OH mitgearbeitet und legt sie bei den datenschutzrechtlichen Prüfungen von Videoüberwachungen in Thüringen zugrunde. Dort sind die Anforderungen an eine datenschutzgerechte Videoüberwachung niedergelegt. Weiterhin gibt es einige Ausführungen zu Spezialfällen, wie beispielsweise zu Webcams, zur Videoüberwachung in Gaststätten, Videoüberwachung von Beschäftigten und zur Videoüberwachung durch Vermie-

ter. Am Ende findet sich eine Checkliste für den Betreiber einer Videoüberwachung öffentlich zugänglicher Räume. Anhand einer Frageliste kann geprüft werden, ob eine datenschutzgerechte Videoüberwachung möglich ist. Falls noch Zweifel bestehen, kann immer noch die Aufsichtsbehörde gefragt werden, da das Ausfüllen der Checkliste keine Garantie für die Rechtmäßigkeit der Überwachungsmaßnahme enthält.

Im Berichtszeitraum stellte sich schnell heraus, dass es weitere Sonderprobleme der Videoüberwachung gibt. Die Ad-hoc-AG wurde daher verstetigt und tagt nunmehr regelmäßig. Sie hat für zwei weitere Bereiche potentieller Videoüberwachung Regelungen getroffen. Zum einen wurde die OH „Videoüberwachung in öffentlichen Verkehrsmitteln“ erarbeitet und vom Düsseldorfer Kreis mit Stand vom 16. September 2015 beschlossen, zum anderen wurde ein Zusatz zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ zur Videoüberwachung in Schwimmbädern erarbeitet. Dieser Zusatz ist unter https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/01_zusatz_zur_oh_v__.pdf auf der Homepage des TLfDI veröffentlicht. In dem Zusatz werden ergänzend zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ spezielle Probleme, die in Schwimmbädern auftauchen datenschutzrechtlich beurteilt. Bereits in seinem 9. Tätigkeitsbericht zum Datenschutz im öffentlichen Bereich hatte der TLfDI unter Nr. 5.5 über die Schwierigkeiten bei datenschutzrechtlichen Kontrollen in Frei- und Hallenbädern berichtet. Nunmehr liegen auch hier bundeseinheitliche Anforderungen vor und der TLfDI kann bei seinen Prüfungen nun die mit den anderen Aufsichtsbehörden abgestimmten Anforderungen anwenden.

Die AG Videoüberwachung hat unter Mitarbeit des TLfDI die OH „Videoüberwachung durch nicht-öffentliche Stellen“ erarbeitet, mit der nunmehr bundeseinheitliche Anforderungen für die datenschutzrechtliche Zulässigkeit einer Videoüberwachung vorliegen. Ergänzt wird diese OH durch einen Zusatz für die Videoüberwachung in Schwimmbädern und mit der OH „Videoüberwachung in öffentlichen Verkehrsmitteln“. Alle potentiellen Betreiber einer

Videoüberwachungsanlage sind gut beraten, sich zunächst mit den dort niedergelegten Anforderungen vertraut zu machen.



Schilder Datenaustausch zwischen USA und EU – © kamasigns / Fotolia.com

3 Europäischer und Internationaler Datenschutz

3.1 Safe Harbor – Anlegen verboten

Der 6. Oktober 2015 war ein guter Tag für den Datenschutz. Die Luxemburger Richter des Europäischen Gerichtshofes (EuGH) urteilten, dass die Entscheidung der Europäischen Kommission vom 26. Juli 2000 (2000/520/EG) über die Gewährung eines angemessenen Datenschutzniveaus auf der Grundlage des Safe-Harbor-Abkommens (Übersetzung wörtlich: „Sicherer-Hafen-Abkommen“) für Übermittlungen von Daten in die USA keine Gültigkeit mehr besitze (Az.: C-362/14).
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowie die anderen Datenschutzbeauftragten des Bundes und der Länder hatten bereits nach den Enthüllungen von Edward Snowden im Sommer 2013 immer wieder die Aussetzung der Übermittlung personenbezogener Daten auf der Grundlage des Safe-Harbor-Abkommens gefordert, da nach Ansicht der deutschen Datenschutzbeauftragten das Abkommen keinen ausreichen-

den Schutz vor Eingriffen in das Grundrecht auf informationelle Selbstbestimmung durch die amerikanischen (Sicherheits-)Behörden biete. Die USA verfügten demnach nicht über ein für europäische Standards notwendiges angemessenes Datenschutzniveau. Dies wurde nunmehr durch die Richter des EuGH bestätigt. Als Folge des Urteils wird der TLfDI zunächst die Übermittlung von personenbezogenen Daten, die sich ausschließlich auf das Safe-Harbor-Abkommen stützen, untersagen und gegebenenfalls mit den ihm zur Verfügung stehenden Mitteln ahnden.
Im Lichte des EuGH-Urteils sind aber darüber hinaus auch die Datenübermittlungen in die USA, basierend auf EU-Standardvertragsklauseln oder so genannten verbindlichen Unternehmensregelungen (auf Englisch: Binding Corporate Rules (BCR)) höchst fraglich geworden. In jedem Fall werden die deutschen Datenschutzbehörden keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von BCR oder Datenexportverträgen erteilen. Zu klären ist auch, ob und inwieweit Datenübermittlungen aufgrund einer Einwilligung der Betroffenen vorgenommen werden können.
Der EuGH stellte in seinem Urteil weiter fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten unabhängig von der Entscheidung der Kommission nicht daran gehindert sind, die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen. Schwierig wird es jedoch, die Entscheidungen der Kommission rechtlich anzugreifen, da den Datenschützern bisher kein eigenes Klagerecht zur Verfügung steht. Hier ist – so der EuGH – der Gesetzgeber gefordert, ein entsprechendes Klagerecht gesetzlich zu verankern.
Diese und weitere Punkte wurden auf einer Sondersitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) am 21. Oktober 2015 in einem Positionspapier zusammengetragen (siehe Anlage 68).
Die „Schonfrist“ für Unternehmen, ihre Arbeitsabläufe entsprechend datenschutzkonform anzupassen bzw. neu zu regeln, lief bis zum 31. Januar 2016 und wurde dann noch einmal bis zum 29. Februar 2016 verlängert. Das mittlerweile von der EU-Kommission vorgelegte geplante Privacy-Shield-Abkommen wird aber nicht nur von der Artikel 29-Datenschutzgruppe als dringend nachbesserungswürdig erachtet. Die Kompetenzen und die Unabhängigkeit einer Ombudsperson für datenschutzrechtliche Belange von EU-Bürgerinnen und Bürgern in den USA erscheint dabei

ebenso fraglich wie die weiterhin mögliche massenhafte Datenspeicherung durch US-Geheimdienste. Stürmische Zeiten im Datenschutzrecht bleiben uns daher wohl erhalten.

Mit dem Safe-Harbor-Urteil hat der Europäische Gerichtshof eine klare Linie aufgezeigt. Datenübermittlungen in die USA auf der Grundlage des Safe-Harbor-Abkommens sind unzulässig. Insbesondere Unternehmen sollten nun schnellstmöglich ihre Verfahren zum Datentransfer überprüfen und datenschutzgerecht gestalten. Inwieweit Datenübermittlungen auf der Grundlage von EU-Standardvertragsklauseln, BCR oder aufgrund der Einwilligung der Betroffenen weiterhin zulässig sind, wird sich im Jahr 2016 zeigen.

3.2 Die Datenschutzgrundverordnung: Trilog beendet und alles auf Anfang!

DSGVO – wissen Sie, was sich hinter dieser ominösen Abkürzung versteckt? Nein? Aufklärung ist in jeder Hinsicht dringend geboten: Diese Abkürzung steht für die Datenschutzgrundverordnung – im Amtsdeutsch der Europäischen Union (EU) auch „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung)“ genannt. Das Ausmaß dieser neuen Regelung ist den meisten Bürgern bisher ebenso unbekannt wie vielen Betrieben und Behörden. Dennoch soll die DSGVO im wahrsten Sinne „für alle“ gelten, denn zum ersten Mal vereint sie ein Regelwerk, dass sowohl im öffentlichen Bereich, also für Landes- und Kommunalbehörden, als auch im nicht-öffentlichen Bereich, also für Betriebe, unmittelbare Anwendung findet. Die DSGVO soll die „alte“ Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 ablösen und unmittelbar in allen Mitgliedstaaten der EU gelten.
Rückblende: Die Vorarbeiten für die Entstehung einer DSGVO reichen bis ins Jahr 2012 zurück. Zuerst erarbeitete die Europäische Kommission einen Vorschlag für eine DSGVO (Vorschlag vom 25. Januar 2012 KOM[2012]11 endgültig; 2012/0011 [COD]) es folgte ein Beschluss des Europäischen Parlaments vom 12. März 2014. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) begleitete bereits diese Phase des Entstehungsentwurfs, indem sie in Form von zwei Entschließungen

zum Gesetzgebungsverfahren Stellung bezog (siehe dazu die Entschließungen vom 28. März 2014 und 19. März 2015 in der Anlage 5 und 21).
Schließlich legte der Rat der Europäischen Union am 15. Juni 2015 seine Vorschläge für eine DSGVO auf den Tisch. Direkt im Anschluss daran begann das so genannte Trilog-Verfahren. Ziel dieses Verfahrens war es, eine Einigung auf eine Fassung aus den unterschiedlichen DSGVO-Entwürfen von Kommission, Parlament und Rat zu erarbeiten. Auch hier brachte die DSK ihre Forderungen an das Trilog-Verfahren auf den Punkt, indem sie das Papier „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung vom 29. Juli 2015 verabschiedete. Die Einigung im Trilog-Verfahren gelang tatsächlich in genau einem halben Jahr: Am Abend des 15. Dezembers 2015 präsentierten die Verhandlungsführer der drei genannten EU-Einrichtungen ihren Kompromissvorschlag. Dieser ist in folgenden Punkten zu begrüßen:

- Ein Recht auf Vergessenwerden (Art. 17 DSGVO) garantiert Betroffenen, dass sie künftig bei der Durchsetzung ihres Löschungsanspruchs gegenüber Dritten stärkere Unterstützung von der verantwortlichen Stelle als bisher erhalten.
- Das so genannte One-Stop-Shop-Verfahren soll die Durchsetzung der Betroffenenrechte erleichtern, indem sich der Betroffene künftig an die Datenschutzaufsichtsbehörde seines Bundeslandes wenden kann, wenn er seine personenbezogenen Daten auch in einem anderen (Bundes-) Land unrechtmäßig verarbeitet sieht.

Wo Licht ist, ist bekanntlich auch Schatten – aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) sind folgende Regelungen der DSGVO nicht besonders geglückt bzw. hätten deutlicher im Sinne des Datenschutzes formuliert werden müssen:

- Nicht genutzt haben die Beteiligten des Trilog-Verfahrens die Chance, stillschweigende oder konkludente Einwilligungen als Voraussetzung für eine Verarbeitung personenbezogener Daten auszuschließen. Eine ausdrückliche Einwilligung ist auch künftig nur für die Verarbeitung besonders sensibler personenbezogener Daten erforderlich.

- Ebenso fehlt in der DSGVO eine ausdrückliche Regelung des Grundsatzes der Datensparsamkeit. Einer solchen Regelung hätte es aber bedurft, wenn die EU der Verwendung von Big-Data-Technologien effizient hätte begegnen wollen.
- Ferner enthält die DSGVO keine ausreichend detaillierte Regelung, die die Profilbildung wirksam begrenzt. Dies ergibt sich bereits aus der Überschrift des in Rede stehenden Art. 20 DSGVO, die da lautet: „Automatisierte Generierung von Einzelentscheidungen einschließlich Profiling“.

Da die DSGVO als Minimalkonsens betrachtet werden muss, enthält sie so genannte Öffnungsklauseln, die es den Mitgliedstaaten der EU – also auch der Bundesrepublik Deutschland – gestatten, durch gesonderte Normen im nationalen Recht bestimmte datenschutzrechtliche Aspekte weitergehender oder strenger zu regeln. Dies betriff vor allem:

- die Öffnungsklausel zur Benennung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich, also in Betrieben (Art. 35 Abs. 4 DSGVO). Bereits das Bundesdatenschutzgesetz (BDSG) sieht in § 4f Abs. 1 Satz 1 eine Pflicht zur Bestellung eines Datenschutzbeauftragten in Betrieben vor. Da eine solche Verpflichtung nicht in die DSGVO aufgenommen wurde, bleibt es künftig dabei, dass in der Bundesrepublik Deutschland im nicht-öffentlichen Bereich Datenschutzbeauftragte nur aufgrund nationalen Rechts zu bestellen sind. Dies setzt aber voraus, dass der Bundesgesetzgeber eine solche Verpflichtung zur Bestellung eines Datenschutzbeauftragten in Betrieben in das Gesetz, das das BDSG ablösen wird, aufnimmt;
- die Öffnungsklausel zur Regelung des Beschäftigtendatenschutzes (Art. 82 Abs. 1 DSGVO). Dabei geht es darum, wie die personenbezogenen Daten des Arbeitnehmers aus seinem Beschäftigungsverhältnis zum Arbeitgeber geschützt oder unter welchen Voraussetzungen sie verarbeitet werden dürfen;
- die Öffnungsklausel zur Verarbeitung sensibler Daten (Art. 9 Abs. 1 und Abs. 4 DSGVO), wonach die Mitgliedstaaten bestimmen dürfen, wann, von wem und unter welcher Geheimhaltungspflicht besonders sensible personenbezogene Daten, wie z. B. Daten, aus denen politische oder religiöse Überzeugungen

hervorgehen, genetische oder biometrische Daten sowie Daten über Gesundheit oder Sexualleben, verarbeitet werden dürfen;
- Die Öffnungsklausel zur Beschränkung subjektiver Datenschutzrechte (Art. 21 DSGVO) erlaubt den Mitgliedstaaten, die Rechte und Pflichten aus den Artikeln 12 bis 20, Artikel 32 und Artikel 5 DSGVO im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte achtet und zum Schutz der nationalen Sicherheit, zur Landesverteidigung, zum Schutz der öffentlichen Sicherheit oder zur Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung dient.

Als große Herausforderung für alle deutschen Datenschutzbeauftragte, aber auch die übrigen Datenschutzbehörden in der EU ist das völlig neu geschaffene Kohärenzverfahren (Artikel 57 ff. DSGVO) anzusehen. Dieses regelt erstmals, wie sich die zuständigen Datenschutzbehörden untereinander und mit dem Europäischen Datenschutzausschuss zu verständigen haben, wenn zum Beispiel ein großer europäischer Konzern mit Hauptsitz in einem EU-Mitgliedstaat und Niederlassungen in mehreren anderen EU-Mitgliedstaaten verbindliche unternehmensinterne Datenschutzvorschriften zur Anwendung bringen will, die von der federführenden Aufsichtsbehörde nach § 43 DSGVO zu genehmigen sind.
Spannend zu beobachten wird es schließlich sein, inwiefern die deutsche Bundesregierung bis zur Bundestagswahl im Herbst 2017 imstande sein wird, diese Öffnungsklauseln „mit Leben zu füllen“ und insgesamt ein Rahmengesetz zur DSGVO als Nachfolgesetz zum BDSG auf den Weg zu bringen.
In einem solchen Gesetz wird sich sehr wahrscheinlich auch eine Regelung wiederfinden, welche deutsche Datenschutzbehörde die Bundesrepublik Deutschland im neu einzurichtenden Europäischen Datenschutzausschuss vertreten darf.
Am 14. April 2016 hat das Europäische Parlament die DSGVO verabschiedet. Nach anschließender Veröffentlichung der DSGVO im Amtsblatt der EU wird diese sehr wahrscheinlich noch im Mai 2016 in Kraft treten.
Anschließend bleibt allen Anwendern dieses neuen Regelungswerkes eine Übergangsfrist von zwei Jahren, sodass die DSGVO spätestens im Frühjahr 2018 für alle Betroffenen anzuwenden ist. Der TLfDI wird diesen Einführungs- und Anwendungsprozess intensiv begleiten

und steht im Rahmen seiner personellen Möglichkeiten mit Rat und Tat bei Fragen zur Verfügung.

Spätestens ab Frühling 2018 wird es „ernst“: Dann ist die DSGVO zwingend für alle Behörden und Betriebe unmittelbar geltendes Recht. Die bisherigen Regelungen des Thüringer Datenschutzgesetzes (ThürDSG) und auch des BDSG haben dann „ausgedient“; Rahmengesetze auf Bundes- und Landesebene werden aber weiterhin erforderlich sein, allein deshalb, um die zahlreichen Öffnungsklauseln der DSGVO, die Sonderregelungen im nationalen Recht erlauben, in einem Gesetz zusammenzufassen. Der Datenschutz wird also nicht einfacher, aber auch nicht langweiliger …

3.3 Die JI-Richtlinie – war da was?

Großen Beratungs- und Gesprächsbedarf verursachte im Berichtszeitraum des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Datenschutzgrundverordnung (DSGVO) (siehe dazu Nummer 3.2). Ein unbedeutendes Schattendasein im Vergleich dazu fristete die so genannte JI-Richtlinie – wobei der Buchstabe J für Justiz und der Buchstabe I für Inneres steht. Die korrekte Bezeichnung dieser Richtlinie lautet: „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“.
Das Ziel dieser Richtlinie ist gemäß ihres Artikels 1 Abs. 1 die Aufstellung von „Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt.“
Dass der JI-Richtlinie keine große Beachtung in der Öffentlichkeit geschenkt wurde, lag zum einen daran, dass sie von der Kommission bereits am 25. Januar 2012 sozusagen „im Doppelpack“ mit der DSGVO vorgestellt wurde und ab Herbst 2015 dann auch im Trilog-Verfahren wieder zusammen mit der DSGVO beraten wurde. Deshalb war es auch nicht weiter verwunderlich, dass sowohl der Stand-

punkt des Europäischen Parlaments zur JI-Richtlinie vom 12. März 2014 (Dok. 7428/14) als auch die allgemeine Ausrichtung des Rates (Dok. 12555/15) zu der JI-Richtlinie nahezu unbemerkt geblieben sind. Vielleicht lag es aber auch am „dünnen“ Regelungsgehalt dieses Richtlinienentwurfs. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) richtete daher am 29. Oktober 2015 (siehe dazu das Eckpunktepapier „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutzrichtlinie im Bereich von Justiz und Inneres“ in der Anlage 68) in einem umfassenden Eckpunktepapier folgende Forderungen an das Trilog-Verfahren:

- Die DSK sah die vom Rat geforderte Erweiterung des Anwendungsbereichs der JI-Richtlinie zulasten der DSGVO kritisch und forderte eine konsequente Trennung des Anwendungsbereichs beider Regelungswerke.
- Die DSK forderte, dass eine strengere Zweckbindung der Daten gewährleistet werden muss und regte an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung personenbezogener Daten zu machen.
- Die DSK mahnte an, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen und kürzeren Fristen als im Entwurf der JI-Richtlinie vorgesehen, gespeichert werden dürfen.
- Die DSK forderte als Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen.
- Die DSK verlangte umfassende Benachrichtigungspflichten zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtschutzes.

Diesen und weiteren Forderungen der DSK wird die im Trilog-Verfahren ausgearbeitete Endfassung der JI-Richtlinie nur im Ansatz gerecht. Das Problem der Zweckbindung hat man in Artikel 4 Abs. 2 der JI-Richtlinie dergestalt gelöst, dass eine Verarbeitung personenbezogener Daten für andere Zwecke dann erlaubt sein soll, wenn der zur Verarbeitung Verantwortliche nach Unions- oder einzelstaatlichem Recht befugt ist, die Daten für diesen anderen Zweck zu verarbeiten und ferner das Unions- oder einzelstaatliche Recht die Daten-

verarbeitung für diesen anderen Zweck als erforderlich und verhältnismäßig erachtet.
Dieses Beispiel aus Artikel 4 Abs. 2 der JI-Richtlinie offenbart eine ihrer Hauptschwächen: Ihrer Zielsetzung, ein zentrales Regelungswerk für den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit zu schaffen, wird die JI-Richtlinie nicht gerecht. Dies verhindern allein schon die vielen Öffnungsklauseln, die den Mitgliedstaaten eine nationale Regelungsmöglichkeit offerieren.
Eine weitere Regelung, die zu weniger statt zu mehr Rechtsklarheit im Bereich des Datenschutzes führen wird, ist Artikel 59 der JI-Richtlinie: Dieser bestimmt, dass besondere Bestimmungen zum Schutz personenbezogener Daten, die in vor Erlass dieser Richtlinie im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, von der JI-Richtlinie unberührt bleiben sollen. Das bedeutet: Der speziellere Rechtsakt, der vor der JI-Richtlinie in Kraft getreten ist, verdrängt diese in ihrer Anwendung. Das erhöhte Prüfaufkommen in Polizei und Justiz, welches EU-Regelungswerk, das der JI-Richtlinie zeitlich vorausgegangen ist, spezieller als diese ist, darf man sich bereits jetzt konkret ausmalen.
Angesichts dieser fragwürdigen Fortschritte, die die JI-Richtlinie für Polizei und Justiz im Bereich des Datenschutzes bereithält, fragen sich nicht wenige Datenschützer und Rechtsprofessoren, ob das „wirklich Neue“ des Regelungswerkes nicht darin zu sehen ist, was nicht in der Richtlinie zu Papier gebracht worden ist: die Anwendung der Grundrechte aus der Charta der Grundrechte der EU (GR-Charta) auch auf deutsche Straf- und Polizeigesetze gemäß Art. 51 GR-Charta. Denn da die nationalen Gesetze nunmehr auch von der JI-Richtlinie berührt werden, wirken die Grundrechte der GR-Charta auf diese Normen der Mitgliedstaaten ein. Das hätte für die Bundesrepublik Deutschland zur Folge, dass sich künftig nicht mehr nur das Bundesverfassungsgericht und die Verfassungsgerichte der Länder, sondern auch der Europäische Gerichtshof in Luxemburg mit der Frage beschäftigen könnten, ob deutsche Straf- und Polizeigesetze gegen Grundrechte verstoßen.
Mit der Umsetzung dieser Richtlinie in deutsches Recht wird sich beim TLfDI unter anderem eine Polizistin beschäftigen, die seit Ende März 2016 für insgesamt sechs Monate von der Thüringer Landespolizeidirektion abgeordnet worden ist.

Neue Datenschutzregelungen „im Doppelpack“: Zusammen mit der Verabschiedung der DSGVO ist auch die Beschlussfassung über die JI-Richtlinie im Europäischen Parlament voraussichtlich im Juni 2016 geplant. Die Prüfung, welche Rechtsnormen in den nationalen Straf- und Polizeigesetzen aufgrund der JI-Richtlinie zu novellieren sind, könnte dabei recht schnell erfolgen. Denn aufgrund der zahlreichen Öffnungsklauseln in der JI-Richtlinie, kann jeder Mitgliedstaat auch künftig seine „datenschutzrechtlichen Extrawürste“ im Bereich von Polizei und Justiz „braten“. Eine Chance für eine europäische Rechtsangleichung auf dem Gebiet des Datenschutzes wurde mit der JI-Richtlinie jedenfalls vertan.

internet – © Julien Eichinger / Fotolia.com

4 Neue Medien – Rundfunk – Telekommunikation

4.1 Melderegisterdaten für ARD, Günter Jauch und Co.?

Eine Bürgerin wandte sich mit „Fragen zur Widerspruchsmöglichkeit gegen die Weitergabe von Daten durch die Meldebehörde" an den TLfDI: Sie habe sich informiert und nirgends etwas darüber gefunden, dass die Meldebehörde ihre Daten zwecks Gebührenerhebung an Rundfunk und Fernsehen schicken dürfe. Sie ärgere insbesondere, dass der Beitragsservice (ARD ZDF Deutschlandradio Beitragsservice) diese Daten ohne ihr Wissen bzw. entsprechende Aufklärung erhalte. Infrage stand für sie, ob sie den Gebührenforderungen des Beitragsservices nunmehr nachkommen

müsse oder ob sie sich ggf. darauf berufen könne, dass die Datenübermittlung unzulässig sei und die Gebührenforderung deshalb als eine Art Werbung angesehen werden könne. Als „kleiner Bürger“ wolle sie zudem nicht für die Gagen von Herrn Günter Jauch und Co. aufkommen.
Der TLfDI hat die Bürgerin hinsichtlich des Verfahrens der Gebührenbeitreibung mittels Meldeamtsdaten informiert und auf den Beschluss des Oberverwaltungsgerichts Lüneburg verwiesen (Az. 4 ME 204/13). Darin hatten die Richter festgestellt, dass der durch den Beitragsservice vorgenommene Abgleich der Melderegisterdaten mit dem beim Beitragsservice vorhandenen Datenbestand auf Grundlage des Rundfunkbeitragsstaatsvertrags erforderlich sei und damit keinen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung darstelle. Gegen diese Rechtsprechung kann auch der TLfDI nichts unternehmen. Im Ergebnis hat der TLfDI die Bürgerin darüber informiert, dass ein Widerspruch gegen diesen Datenabgleich mit dem Beitragsservice (wegen Rundfunk- und Fernsehgebühren) nicht erfolgversprechend ist.

Der TLfDI hilft, wo er kann, um das Grundrecht auf informationelle Selbstbestimmung durchzusetzen. Sofern ein Gericht aber entschieden hat, dass dieses Grundrecht – wie im Fall des Meldedatenabgleichs mit dem aktuellem Datenbestand des Beitragsservices von ARD, ZDF und Deutschlandradio – nicht verletzt ist, hilft es dem Bürger nicht weiter, wenn der TLfDI ihm eine davon abweichende Rechtsauffassung nahelegt und der Bürger vor einem Gericht mit dieser Rechtsauffassung scheitern würde.

4.2 Löschung von Google-Suchergebnissen

Das Internet vergisst nie. So sind eingestellte Informationen im Internet über Jahre abrufbar, werden oft sogar weiter kopiert und woanders erneut sichtbar gemacht. Um Informationen im Internet zu finden, bedient man sich so genannter Suchmaschinen, als Beispiel sei hier die Suchmaschine von Google Inc. genannt. Welches Suchergebnis Suchmaschinen im Internet bei der Suche nach einem Begriff oder Namen anzeigen, bestimmt sich dabei in der Regel nach den kommerziellen Interessen der Suchmaschinenbetreiber und ihrer Vertragspartner.

Nun gibt es Fälle, in denen man nicht – oder nicht mehr – möchte, dass bestimmte Informationen über einen selbst auffindbar sind. Diese Informationen lassen sich allerdings nur löschen, wenn man sich direkt an den Betreiber der jeweiligen Webseite wendet, wo diese Informationen eingestellt sind. Ein Löschantrag über den Provider der Webseite ist in der Regel wenig erfolgreich. Oft bleiben aber beide Wege erfolglos, u. a. weil der Ansprechpartner seinen Sitz nicht in Deutschland bzw. im Europäischen Raum hat. Also lag die Idee nahe, wenn man schon nicht die Quellen löschen kann, dann wenigstens auf das Ergebnis von Suchmaschinen Einfluss zu nehmen.

So hatte der Europäische Gerichtshof am 13. Mai 2014 (C-131/12) Google Inc. dazu verpflichtet, auf Antrag bestimmte Suchergebnisse (Links) aus seinen Suchergebnislisten zu entfernen. Dies allerdings nur, wenn ein begründeter Widerspruch vorliegt und die Datenschutzrechte der betreffenden Person schwerer wiegen als das Interesse an der Verfügbarkeit der betreffenden Suchergebnisse.

Zudem darf der Europäische Gerichtshof nur Recht für die Europäische Union aussprechen. Die gleiche Suche mit Google – bspw. in den USA gestartet – zeigt weiterhin alle Treffer an.

So hat die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 in ihrer Entschließung „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ auch darauf hingewiesen, dass aufgrund der territorialen Unbeschränktheit des Internets auch der Schutz des Einzelnen universell gelten muss (s. Link https://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/dsk_google_suchergebnisse.pdf). Das bedeutet, eine Beschränkung nur auf den Europäischen Raum ist für die Betroffenen derzeit nicht in jedem Fall zielführend.

Sollte man dennoch einen Antrag auf Entfernung von Suchergebnissen bei Google Inc. stellen wollen, muss man zunächst das begründete Löschbegehren direkt an Google Inc. richten. Dieses Antragsformular ist zu finden unter:

https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de

Nach Antragstellung wird dann u. a. die Identität geprüft. Dies bedeutet, Google Inc. möchte einen Nachweis der Identität. Aus datenschutzrechtlicher Sicht sollten hierfür keine Kopien vom Personalausweis oder Reisepass verwendet werden! Man kann bspw. den Bibliotheksausweis oder andere Dokumente verwenden. Zudem empfiehlt es sich, generell zuvor auf der Kopie des zu sendenden Dokumentes alle Angaben (Zahlen), die nicht unmittelbar mit der Person zu tun haben, zu löschen.

Wird der hinreichend begründete Löschantrag von Google Inc. abgelehnt, kann man sich danach an die zuständige Aufsichtsbehörde, den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, wenden. Neben der Nennung des Suchbegriffes, des konkret zu löschenden Links und der geführten Kommunikation mit Google Inc., ist auch dessen vergebene Bearbeitungsnummer (Ticketnummer) mit zu übersenden.

Anträge auf Entfernen von Suchergebnissen bei Google sind direkt an Google Inc. zu stellen. Ein Antrag hat nur Erfolg, wenn eine gewisse Schwere der Persönlichkeitsrechtsbeeinträchtigung nachvollziehbar vorliegt. Bei der notwendigen Kopie eines zu identifizierenden Dokumentes sollte keine Kopie vom Personalausweis oder Reisepass verwendet werden, besser ist bspw. der Bibliotheksausweis.
Die Entfernung von Ergebnissen bei einer Suchmaschine bedeutet nicht, dass die eigentlichen Daten gelöscht wurden.

4.3 16 Millionen Zugangsdaten geraubt – was nun?

Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden rund 16 Millionen kompromittierte Benutzerkonten mit E-Mail-Adressen und zugehörigen Passwörtern entdeckt. Benutzerkonten und Passwörter sind oft Angriffsziele im Rahmen der Cyber-Kriminalität (Cyberattacken). Sie werden nicht nur missbraucht, um der betroffenen Person selbst zu schaden (z. B. durch Nutzung der Kennungen

bei Online-Shops und Online-Banking), sondern auch, um an den Nutzer selbst oder unter seinem Namen an andere Nutzer SPAM-Mails zu versenden. Letzteres ist ein beliebter Trick, um Werbung oder Schadsoftware zu verteilen.

Um den Bürgern eine Überprüfungsmöglichkeit einzuräumen, ob sie von diesem „Identitätsdiebstahl“ betroffen waren, wurde die Liste dem Bundesamt für Sicherheit in der Informationstechnik (BSI) übergeben. Das Bundesamt stellte daraufhin eine Webseite zur Verfügung, auf welcher jeder Bürger durch Eingabe seiner E-Mail-Adresse prüfen konnte, ob er vom Diebstahl betroffen war. Diese Seite ist auch weiterhin abrufbar unter: https://www.sicherheitstest.bsi.de/.

Die Idee, den Bürgern zu helfen, ist natürlich aus datenschutzrechtlicher Sicht ein primäres Ziel. Dennoch hat die Verfahrensweise einen gefühlten Beigeschmack. Durch die Eingabe auch nicht betroffener E-Mail-Adressen verunsicherter Bürger gelangt nun das BSI theoretisch an diese zusätzlichen E-Mail-Adressen, auch wenn diese sich gar nicht unter den 16 Millionen Adressen befanden.

Da man sich vor Cyberattacken auf Rechner Dritter (z. B. externe Rechenzentren oder Server in der Cloud), wo auch die eigenen Zugangsdaten gespeichert sind, nicht selbst schützen kann, gilt es, die Auswirkungen von Cyberattacken selbst so gut wie möglich zu minimieren. Deshalb veröffentlichte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) dazu auch eine entsprechende Pressemitteilung: (https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pressemitteilung_tlfdi_21012014.pdf). In dieser werden erste Maßnahmen vorgestellt, wie man als Betroffener reagieren sollte.

Die große Gefahr an einer solchen Diebstahl-Situation ist, dass durch die gestohlenen E-Mail-Adressen und die dazugehörigen Passwörter missbräuchlich Zugänge von unberechtigten Dritten zu Internet-Diensten genutzt werden könnten. Wird dasselbe Passwort auch für andere E-Mail-Adressen oder Internetportale verwendet, können auch diese Zugän-

ge theoretisch unberechtigt genutzt werden. Die Folgen einer solchen Übernahme sind meist schwer abschätzbar. Um nicht erst in eine solche Situation zu geraten, sollte man als Nutzer einige Grundregeln beachten, auf die der TLfDI an dieser Stelle noch einmal hinweisen möchte:

- Nutzen Sie nie dasselbe Passwort in mehreren E-Mail-Adressen oder Internetportalen.
- Bei selten genutzten Internetportalen reichen „Einmalpasswörter". Nach der Nutzung kann man sein Passwort heutzutage auch per Klick neu anfordern bzw. erzeugen lassen.
- Achten Sie auf ausreichend sichere Passwörter. Orientieren Sie sich dabei an der Maßnahme M 2.11 der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der IT (BSI) – d. h. verwenden Sie mindestens acht zufällig gewählte Zeichen inklusive Buchstaben, Zahlen und Sonderzeichen.
- Achten Sie bei der Nutzung eines Passwortverwaltungsprogrammes darauf, dass das Masterpasswort eine außergewöhnlich hohe Sicherheit besitzt, d. h. sehr viele Sonderzeichen, Zahlen und Buchstaben.

Sollten Sie auch nur den Verdacht haben, dass Ihre Zugangsdaten unberechtigten Dritten bekannt sind bzw. von diesen missbraucht werden, wechseln Sie unbedingt sofort alle gleichlautenden Passwörter. Der TLfDI empfiehlt daher, Passwörter grundsätzlich nie doppelt zu verwenden und die Komplexität der Passwörter nach der o. g. Maßnahme des BSI zu gestalten.

4.4 Datenschutz und Medienprivileg

Eine Bürgerin bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), eine Löschung der zu ihrer Familie und ihrer eigenen Person auf einem Internetportal veröffentlichten personenbezogenen Daten durchzusetzen. Die Nachforschungen des TLfDI ergaben, dass ein Journalist Beiträge, die personenbezogene Daten über die Beschwerdeführerin und über ihre bereits verstorbenen Familienmitglieder enthielten, auf diesem Internetportal veröffentlicht hatte. Da weder der Journalist noch das Internetportal als öffentliche Stellen einzuordnen waren, kam für die Beurteilung des Sachverhalts zunächst das Bundesdatenschutzgesetz (BDSG) zur Anwendung. Nach den Regelungen des § 20 Abs. 2

BDSG sind personenbezogene Daten, die automatisiert verarbeitet werden, insbesondere dann zu löschen, wenn ihre Speicherung unzulässig ist. Zu berücksichtigen war vorliegend auch, dass gemäß § 3 Abs. 1 BDSG personenbezogene Daten grundsätzlich nur solche Angaben sind, die sich auf eine natürliche Person beziehen. Jeder lebende Mensch ist eine natürliche Person. Für Verstorbene fehlt im BDSG eine ausdrückliche Regelung. Die Würde des Menschen ist nach Artikel 1 Abs. 1 des Grundgesetzes grundsätzlich auch über den Tod hinaus zu respektieren. Daher kann eine Veröffentlichung nach dem Tod die Würde eines Verstorbenen unter Umständen beeinträchtigen. Der Wert- und Achtungsanspruch besteht zwar fort, verblasst aber mit der Zeit. So führt das Bundesverfassungsgericht hierzu aus: „Das Schutzbedürfnis schwindet in dem Maße, in dem die Erinnerung an den Verstorbenen verblasst und im Laufe der Zeit auch das Interesse an der Nichtverfälschung des Lebensbildes abnimmt“ (BVerfGE 30, 173 [196]). Da die betroffenen Familienangehörigen der Beschwerdeführerin bereits seit längerer Zeit verstorben waren, bestand in diesem Fall kein Anspruch auf eine Löschung. Eventuell standen der Bürgerin hier zivilrechtliche Abwehr- und Schadensersatzansprüche zu. Dies zu beurteilen lag jedoch nicht in der Zuständigkeit des TLfDI. Auch hinsichtlich der Veröffentlichung von personenbezogenen Daten der Beschwerdeführerin musste der TLfDI feststellen, dass es sich bei dem Internetportal um einen journalistischen Auftritt handelte. Die für den Portalauftritt verantwortliche Stelle war Mitglied im deutschen Presserat. Die Seite fungierte nach dem zugrundeliegenden Konzept als Nachrichtenportal für einige Regionen in Thüringen. Nach § 41 BDSG haben die Länder in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a BDSG entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 BDSG zur Anwendung kommen. Es handelt sich bei dieser Vorschrift um das so genannte Medienprivileg. Eine derartige Regelung trifft das Thüringer Pressegesetz. Nach § 1 des Thüringer Pressegesetzes (TPG) ist die Presse frei. Sie unterliegt nur den Beschränkungen, die durch das Grundgesetz zugelassen sind. Die Rechte, die Betroffene haben, wenn über sie presserechtliche Veröffentlichungen erfolgen, finden sich im TPG. So besteht beispielsweise nach § 11 TPG ein

Gegendarstellungsanspruch. Nach § 11a TPG gelten die Bestimmungen des BDSG, wie oben zu § 41 BDSG ausgeführt, nur eingeschränkt. Das bedeutet auch, dass eine Aufsichtstätigkeit des TLfDI nach § 38 BDSG nicht möglich ist und der TLfDI deshalb nicht im Sinne der Beschwerdeführerin tätig werden konnte. Der TLfDI konnte die Bürgerin lediglich darauf verweisen, dass es ihr unbenommen war, mögliche zivilrechtliche oder presserechtliche Ansprüche gegen die veröffentlichende Stelle prüfen zu lassen. Außerdem konnte sie sich wie jedermann beim Presserat über eine redaktionelle Veröffentlichung in Zeitungen, Zeitschriften und Online-Medien beschweren und presseethisch prüfen lassen. Unter https://www.presserat.de/beschwerde/online-beschwerde/ ist ein entsprechendes Beschwerdeformular abgedruckt. Der Deutsche Presserat ist auch unter der Adresse Fritschestraße 27/28 in10585 Berlin zu erreichen.

Bei Unternehmen und Hilfsunternehmen der Presse, die ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken personenbezogene Daten erheben, verarbeiten und nutzen, ist eine datenschutzrechtliche Aufsichtstätigkeit des TLfDI nicht gegeben. Bürger, die sich in diesen Fällen in ihrem Persönlichkeitsrecht beeinträchtigt sehen, können sich an den Presserat wenden und auch zivilrechtliche und presserechtliche Ansprüche gegen die verantwortliche Stelle prüfen lassen.

4.5 Falschparkern auf der Spur – Knöllchen durch die „Wegeheld“-App?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Berichtszeitraum über einen Zeitungsbericht darauf aufmerksam, dass eine Applikation (App) „Wegeheld“ für Smartphones entwickelt worden sei, die es ermögliche, einen Verkehrsverstoß bei den Behörden zu melden. Mit der App werde das Auto eines Verkehrssünders fotografiert und das Bild mit geschwärzten Kennzeichen auf einer interaktiven Straßenkarte hochgeladen. Die E-Mail-Adressen der Ordnungsämter der bislang 100 größten Städte in Deutschland seien in diesem Programm hinter-

legt worden. Mittels der „Wegeheld“-App würden die Ordnungsämter sodann benachrichtigt werden, um tätig zu werden. Auch ein „Anschwärzen“, so der Zeitungsbericht, über Twitter und Facebook sei möglich.
Der TLfDI nahm diesen Bericht zum Anlass, bei den 26 größeren Thüringer Kommunen nachzufragen, ob deren Ordnungsämter diese „Wegeheld“-App bereits nutzten und gegebenenfalls Daten daraus verarbeitet hätten.
Das Ergebnis der TLfDI-Umfrage war datenschutzrechtlich erfreulich: Keine der 26 angefragten Kommunen hatte bisher Daten von oder im Zusammenhang mit der „Wegeheld“-App verarbeitet. Einigen Kommunen war die besagte App nicht einmal bekannt.

Damit keine Missverständnisse aufkommen: Der TLfDI will keine „Lanze brechen“ für Falschparker und Raser; ihm kommt es ganz allein auf eine ordnungsgemäße Verarbeitung von personenbezogenen Daten an. Diese ist nur gemäß § 4 Abs. 1 Satz 1 ThürDSG zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlauben oder soweit der Betroffene (hier der durch die „Wegeheld“-App erfasste Autofahrer) seine Einwilligung erteilt hat. Obwohl in Thüringen bisher kein Ordnungsamt die genannte App benutzt hat, geht der TLfDI bisher davon aus, dass die Voraussetzungen für eine solche Datenerhebung nach § 4 Abs. 1 Satz 1 ThürDSG nicht vorliegen dürften.

4.6 Facebook-Fanpage – seit Safe-Harbor-Entscheidung Rechtmäßigkeit noch unsicherer

Im 10. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde unter Punkt 4.3 zum Sachstand der Rechtmäßigkeit des Betreibens von Fanpages bei Facebook berichtet. Die Datenschutzbeauftragten des Bundes und der Länder vertraten mit der Entschließung der 82. Datenschutzkonferenz im September 2011 die Auffassung, dass öffentliche Stellen keine Fanpage einrichten sollten, da hierfür die Rechtsgrundlage fehlt und keine Möglichkeit gesehen wird, eine solche Fanpage datenschutzkonform zu gestalten. Datenschutzrechtlich bedenklich ist dabei die Tatsache, dass beim Ansehen einer Facebook-Fanpage – auch von Nicht-Facebook-Mitgliedern – von Facebook Informationen der Besucher erfasst werden, Facebook also

ein Cookie setzt und Informationen an sich weiterleitet. Welche Daten diese Informationen beinhalten, wollte Facebook bisher nicht transparent offenlegen.
Das Unabhängige Datenschutzzentrum Schleswig Holstein (ULD) leitete sogar gegen drei Unternehmen, die Fanpages betreiben, ein Verfahren ein. Dies mag für den normalen Bürger unverständlich wirken. Dennoch muss tatsächlich die Frage rechtlich geklärt werden, ob jemand eine Fanpage einrichten darf, wissentlich, dass seine Besucher von Facebook erfasst/getrackt werden, Daten also an die USA übermittelt werden. Mittlerweile liegt dieser Rechtsstreit beim Bundesverwaltungsgericht und sollte am 17. Dezember 2015 behandelt werden. Das Verfahren wurde am 25. Februar 2016 vom Bundesverwaltungsgericht ausgesetzt, weil dem Gerichtshof der Europäischen Union sechs Rechtsfragen zur Beantwortung vorgelegt wurden. Es scheint unwahrscheinlich, dass hier eine nationale Lösung erfolgt. Kundige Beobachter und Datenschützer vermuten und hoffen sogar, dass hier eine europäische Lösung angestrebt wird, sodass es nicht unwahrscheinlich erscheint, dass der Europäische Gerichtshof sich damit befassen muss, also es an diesen vom Bundesverwaltungsgericht zwecks Klärung weitergeleitet wird.
Unabhängig davon gab es in Thüringen eine Reihe von Anfragen zum Betreiben von Fanpages an den TLfDI von Landes- und Kommunalbehörden. Aus diesem Grund schaltete der TLfDI bereits im Dezember 2014 eine Pressemitteilung zum Sachstand und gab entsprechende Hinweise (siehe dazu die Anlage 44). Zudem ist die Empfehlung, bis zur endgültigen Entscheidung durch das Bundesverwaltungsgericht auch weiterhin vom Betreiben von Fanpages abzusehen.
Außerdem wandte sich der TLfDI im Dezember 2014 sowohl an den Thüringer Landkreistag und an den Thüringer Gemeinde- und Städtebund und empfahl diesen, bis zur endgültigen rechtskräftigen Entscheidung auch weiterhin vom Betreiben von Fanpages abzusehen.
Anfang 2015 lud der TLfDI diesbezüglich auch die obersten Landesbehörden zu einem Gespräch ein. In diesem Gespräch empfahl der TLfDI bei bereits bestehender Fanpage keine Fotos ohne Einwilligung des Betroffenen zu veröffentlichen und die Kommunikationsmöglichkeiten auf ein Minimum zu beschränken. Der TLfDI erkennt die Begehrlichkeiten und die anscheinende Notwendigkeit, in allen sozialen Netzwerken präsent sein zu wollen, um recht viele Bürger ansprechen zu können.

Datenschutzrechtlich gesehen ist es derzeit jedoch empfehlenswerter, bei sozialen Netzwerken, insbesondere bei Facebook, nur eine Startseite zu betreiben und dann auf die eigene Homepage zu verlinken. Dies würde nicht nur einen erheblichen doppelten Aufwand an Öffentlichkeitsarbeit minimieren, sondern auch der notwenigen Datensparsamkeit Rechnung tragen.
Im Ergebnis kann weiterhin nicht ausgeschlossen werden, dass ein Gericht entscheidet, dass keine Fanpage bei Facebook betrieben werden darf, solange Facebook nicht offenlegt, welche Daten tatsächlich von Besuchern der Fanpage erfasst werden.
Unabhängig davon hat der Europäische Gerichtshof (EuGH) mit seinem Urteil vom 6. Oktober 2015 zur Safe-Harbor-Entscheidung der EU-Kommission eine Datenübermittlung von personenbezogenen Daten in die USA für rechtswidrig erklärt (siehe dazu Nr. 3.1.). Im Kontext dieses Urteils sind auch soziale Netzwerke, wie Facebook, und ihre Datenübermittlung neu zu bewerten.

Das Betreiben von Webseiten in sozialen Netzwerken darf nicht gegen den Datenschutz verstoßen. Da weiterhin die Rechtslage der Verantwortlichkeit von im Hintergrund erhobenen Daten von Websites/Portalbetreibern unsicher ist, sollte auf Seiten dieser Art ganz verzichtet werden. Zudem ist das Urteil des Europäischen Gerichtshofes zu Safe Harbor umzusetzen.

4.7 Telemediengesetz (TMG) – zeitgemäß ?

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Die Datenschutzbeauftragten des Bundes und der Länder monierten allerdings in ihrer Umlaufentschließung vom 5. Februar 2015, dass das Telemediengesetz bezüglich des Setzens von Cookies nicht der Europäischen Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) entspricht (siehe dazu Anlage 19). Denn die E-Privacy-Richtlinie gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind nur, wenn der Nutzer dazu seine Einwilligung gegeben hat und auch hinsichtlich der Notwendigkeit der Speicherung eine Information erfolgte. Dieses ist, nach Meinung der Datenschutzbeauftragten, im Telemediengesetz (TMG) nicht umgesetzt, da

§ 15 Abs. 3 TMG regelt, dass der Nutzer nur auf sein Widerspruchsrecht hinzuweisen ist.
Ein weiteres Problem ist, dass mit der fortschreitenden Digitalisierung auch das Bedürfnis nach öffentlichem Zugang im Internet unter Nutzung frei zugänglicher drahtloser Netzwerke (WLANs) besteht. So wurde auch beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage nach der Haftung (Störerhaftung) gestellt und welche Risiken sich damit verbinden. Das Problem dabei ist, dass die „Störerhaftung" dann eintritt, wenn über ein zur Verfügung gestelltes WLAN eine Rechtsverletzung begangen wurde.
Hintergrund für die unsichere Rechtslage sind § 8 Telemediengesetz (TMG) und verschiedene Urteile des BGHs zur Störhaftung. Um im Nachhinein die Störhaftung weitestgehend zu minimieren bzw. gänzlich auszuschließen, bieten viele Anbieter den Internetzugang über WLAN nur mit einem zugewiesenen Account an – oft verbunden mit der Eingabe weiterer Daten. Dies wird z. B. in Hotels, Flughäfen, Zügen, Straßenbahnen, Fernbussen oder auch in Cafés genutzt.
Aufgrund der Störhaftung sind deshalb „offene" WLANs, die ohne Anmeldung einen Zugriff auf das Internet ermöglichen, in Deutschland sehr selten anzutreffen.
Auslöser einer Störhaftung kann bspw. eine Verletzung des Urheberrechts sein, wie beim Filesharing im Video- und Musikbereich.
Gemäß § 8 Telemediengesetz sind von der Haftung als Störer derzeit nur Internet-Provider ausgenommen. Rechtlich ungeregelt ist daher derzeit die Anwendbarkeit des § 8 TMG hinsichtlich der Haftung privater, geschäftsmäßiger und öffentlicher Anbieter.
Dies hat auch die Bundesregierung erkannt und, um die nötige Rechtssicherheit in Haftungsfragen zu verschaffen, am 18. November 2015 einen „Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes" vorgelegt (BT DS 18/6745).
Der TLfDI empfiehlt daher, das Gesetzgebungsverfahren abzuwarten und wird die Probleme weiter im Blick haben.

Das Telekommunikationsgesetz bedarf hinsichtlich der europäischen Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) einer Klarstellung.
Auch sollte das Betreiben frei zugänglicher drahtloser Netzwerke (WLANs) rechtsicher geregelt werden. Dabei sollte auch die Sicher-

heit der Netzwerkanbindung dem aktuellen Stand der Technik entsprechen.

Rathaus – © DOC RABE Media / Fotolia.com

5 Kommunales

5.1 Bloßstellung in der Schankwirtschaft – öffentliche Auslegung von Beschwerdeschreiben

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt Kenntnis darüber, dass der Bürgermeister einer Thüringer Gemeinde, einer Mitgliedsgemeinde einer Verwaltungsgemeinschaft (VG), Kopien seines an das Ordnungsamt der VG gerichteten Beschwerdeschreibens mit darin enthaltenen personenbezogenen Daten in der Gaststätte zur Kenntnisnahme für jedermann ausgelegt haben soll.
Der TLfDI stufte diesen Sachverhalt zunächst als einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 22 Thüringer Datenschutzgesetz (ThürDSG) (Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs), sowie als einen Bruch des Amtsgeheimnisses ein. Der TLfDI bat die VG aber um eine Stellungnahme zu dem Sachverhalt.
Hierzu teilte die VG u. a. mit, dass der Bürgermeister der Gemeinde sich nicht erklären könne, wie das Beschwerdeschreiben an Dritte weitergegeben worden sei. In diesem Zusammenhang legte die VG dar, dass sie den Bürgermeister auf die unbedingte Einhaltung des

Datenschutzes in seiner Gemeinde und auf den verantwortlichen Umgang mit personenbezogenen Daten hingewiesen habe.
Weiterhin teilte die VG mit, dass die Einhaltung des Datenschutzes in den Mitgliedskommunen und die Verantwortung der Bürgermeister für personenbezogene Daten in einer Versammlung der VG thematisiert würden. Ferner wollte die VG alle nachgeordneten Einrichtungen der Kommunen noch einmal datenschutzrechtlich schulen.
Daraufhin teilte der TLfDI dem Beschwerdeführer mit, dass dem TLfDI keine gesetzlichen Befugnisse zur exakten Klärung des tatsächlichen Sachverhalts, wie sie etwa die Staatsanwaltschaft besitze, zur Verfügung stehen. Beurteilungsprobleme ergaben sich für den TLfDI im konkreten Fall dadurch, dass er Kenntnis von zwei plausiblen, sich jedoch widersprechenden Sachverhalten erhielt und weitere Recherchen keine Aussicht auf Erfolg boten. Insbesondere war für den TLfDI nicht aufklärbar, ob der Bürgermeister das Schreiben des Beschwerdeführers an die VG in der Gaststätte zur Kenntnisnahme für jedermann ausgelegt hatte.
In diesem Falle war es mit den Mitteln, die dem TLfDI nach § 37 Abs. 1 ThürDSG zur Verfügung stehen (Auskunfts- und Fragerecht sowie das Recht auf Akteneinsicht), ausgeschlossen, zweifelsfrei festzustellen, ob sich der beschwerdegegenständliche Datenschutzverstoß so zugetragen hat. Daher konnte der TLfDI die Angelegenheit leider nicht abschließend aufklären.

Aufgrund fehlender gesetzlicher Befugnisse sind den Möglichkeiten des TLfDI zur Aufklärung von Sachverhalten gelegentlich Grenzen gesetzt. Dies ist insbesondere dann der Fall, wenn der TLfDI Kenntnis von zwei plausiblen, sich jedoch widersprechenden Sachverhalten erhält und weitere Recherchen keine Aussicht auf Erfolg bieten. In diesen Fällen gibt der TLfDI jedoch Hinweise, wie eine datenschutzkonforme Verarbeitung personenbezogener Daten in jedem Falle zu erreichen ist.

5.2 Jagdbehördliches Lauschen im Nebenzimmer – ausnahmsweise erlaubt – Türen zum Nebenraum sollten grundsätzlich geschlossen werden

Dass ein gutes Gehör nicht nur bei der Jagd, sondern auch bei amtlichen Tätigkeiten von Bedeutung sein kann und ausnahmsweise auch darf, belegt folgender Beschwerdefall:

Ein Jäger hatte sich wegen der Verlängerung seines Bundesjagdscheins in das Landratsamt Saalfeld-Rudolstadt begeben. In der dortigen Unteren Jagdbehörde bemerkte er während des Gesprächs mit einem Mitarbeiter durch die offen stehende Tür des Nebenzimmers Stimmen. Da ein Mithören unberechtigter Dritter nicht auszuschließen gewesen sei, beschwerte er sich daraufhin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Wie das Landratsamt auf Nachfrage des TLfDI mitteilte, hatten sich während des Gesprächs ausschließlich vertretungsberechtigte und damit zuständige Mitarbeiter der Jagdbehörde im Nebenraum aufgehalten. Daher lag eine Übermittlung von personenbezogenen Daten im Ergebnis nicht vor.
Der TLfDI bat das Landratsamt, künftig dafür Sorge zu tragen, dass die Besucher zu Beginn des Gesprächs aufgrund der gebotenen Transparenz über die Möglichkeit des Mithörens der zuständigen Mitarbeiter im Nebenraum mittels geöffneter Tür in Kenntnis gesetzt werden. Ob die Tür geöffnet wird oder bleibt, ist jedoch von der Einwilligung der Besucher abhängig zu machen. Erteilt der Besucher eine Einwilligung, so ist die Tür zum Nebenraum aber auch dann zu schließen, wenn unberechtigte Personen den Nebenraum betreten. Ferner muss der Nebenraum abgeschlossen werden, sobald ihn die dortigen Mitarbeiter verlassen.

In Ausnahmefällen ist ein Mithören von Gesprächen mit Bürgern durch weitere zuständige Mitarbeiter aus einem Nebenraum heraus im Rahmen ihrer Aufgabenerfüllung nach erfolgter Einwilligung der Betroffenen nicht ausgeschlossen. Hierbei sind die Betroffenen über diesen Sachverhalt zu unterrichten und es sind mittels Dienstanweisung Regelungen zu treffen, die eine Kenntnisnahme unberechtigter Dritter ausschließen.

5.3 Facebook als Informationsquelle für Steuerprüfer

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erschrak bei der Meldung einer Tageszeitung, dass städtische Steuerprüfer Daten mit Facebook abgleichen würden. Hintergrund für diesen angeblichen „Datenabgleich“ waren Zweifel der Prüfer an der Zahl verkaufter Eintrittskarten einer Tanzveranstaltung in einer Diskothek.

Um der Sache aus datenschutzrechtlicher Sicht auf den Grund zu gehen, wandte sich der TLfDI an die Stadtverwaltung Weimar und bat sie um eine Stellungnahme.
Die Stadtverwaltung teilte daraufhin mit, dass weder ein Datenabgleich noch ein Datenaustausch zwischen ihr und Facebook erfolgt sei. Die Teilnehmerzahl konnte die Stadtverwaltung auf der frei zugänglichen Facebookseite der betroffenen Diskothek entnehmen. Die Stadtverwaltung teilte mit, dass eben diese allgemein zugänglichen Informationen im Internet zur steuerrechtlichen Überprüfung verwendet werden können.
Auf der entsprechenden Facebookseite konnte man tatsächlich erkennen, wie viele Personen an dieser Veranstaltung teilgenommen haben. Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
§ 92 Abgabenordnung (AO), der nach § 15 Abs. 1 Nr. 3a Kommunalabgabengesetz (ThürKAG) Anwendung findet, erlaubt der Finanzbehörde, dass sie sich der Beweismittel bedienen kann, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält. Die Kenntnisnahme der Teilnehmerzahl war hier ein zulässiges Mittel zur Erfüllung der in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe. Ein Datenschutzverstoß lag somit selbst für den Fall nicht vor, dass es sich um personenbezogene Daten handelte.

Im Datenschutzrecht gibt es eine einfache Grundregel für den Umgang mit personenbezogenen Daten: Entweder ist die Datenverarbeitung (Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen) und -nutzung durch eine Rechtsvorschrift erlaubt oder der Betroffene hat eingewilligt (§ 4 Abs. 1 ThürDSG). § 92 AO, der nach § 15 Abs. 1 Nr. 3a ThürKAG Anwendung findet, kann eine solche Rechtsvorschrift darstellen. Die Finanzbehörde darf sich nach dieser Vorschrift der Beweismittel bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sofern aber die Erforderlichkeit nicht gegeben ist, scheidet diese Norm als Rechtsgrundlage aus. Dann kann eine Datenverarbeitung nur noch aufgrund einer anderen Rechtsvorschrift zulässig sein oder der Betroffene willigt ein.

5.4 Stadt ist neugierig: Wer wohnt in der Seniorenresidenz?

Der Betreiber einer Seniorenresidenz bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Hilfe. Die zuständige Stadtverwaltung verlangte von ihm, eine Auflistung der Heimbewohner mit Angaben ihrer Zimmergröße in qm neben weiteren mietbezogenen Angaben zu übermitteln. Als Grund wurde die Überprüfung der Alten- und Pflegeheime zur bevorstehenden Änderung des Wohngeldgesetzes angegeben.
Auf Anfrage teilte die Stadtverwaltung zur Erklärung dem TLfDI mit, sie bräuchte die Informationen von den Betreibern von Alten- und Pflegeheimen, um sich auf die Änderung des Wohngeldgesetzes einstellen zu können. Dafür benötige sie unter anderem eine Auflistung der Heimbewohner mit Angabe ihrer Zimmergröße in qm. Diese Angaben dienten dem Abgleich bzw. der Aktualisierung der derzeit in der Behörde vorliegenden Angaben bezüglich dieser Wohngeldempfänger.
Als Rechtsgrundlage stützte man sich auf den Amtsermittlungsgrundsatz nach § 20 Zehntes Buch Sozialgesetzbuch (SGB X). Man bediene sich nur der Beweismittel, die nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts erforderlich seien. Die Auflistung der Heimbewohner mit Angabe ihrer Zimmergröße in qm sei so gemeint gewesen, dass nur die Daten der Heimbewohner, für die zu diesem Zeitpunkt ein Wohngeld bewilligt bzw. beantragt war, abgefragt werden sollten. Dies sei auch dem Pflegeheimbetreiber so vermittelt worden, er wolle dies offenbar nicht verstehen. Aus dem Anschreiben an den Betreiber war die Einschränkung auf die Wohngeldempfänger nicht erkennbar. Die Befugnis zur Amtsermittlung bedeutet nicht, dass grundsätzlich ohne konkreten Anlass und ohne Differenzierung Angaben von Dritten verlangt werden können.
Sollten alle Heimbewohner mit den zur Verfügung stehenden Flächen benannt werden, hätte die Behörde abgleichen können, ob sich darunter Wohngeldempfänger befinden. Dann wären allerdings personenbezogene Daten völlig unbetroffener Personen, nämlich auch derjenigen Personen, die kein Wohngeld beziehen, verlangt worden, wozu keine Befugnis nach dem SGB X bestand.
Das Problem kann aber auch nicht dadurch gelöst werden, dass das Pflegeheim lediglich in Bezug auf Wohngeldbezieher befragt wird. Diese sind dem Heim im Zweifel nicht bekannt. Es hätte seinerseits eine Abfrage bei seinen Bewohnern bedurft, wer von ihnen tatsäch-

lich Wohngeld bezieht oder beantragt hatte. Eigene Ermittlungen des Pflegeheimbetreibers diesbezüglich finden jedoch keine Rechtsgrundlage in den sozialgesetzlichen Vorschriften. Die weitere Möglichkeit, dem Pflegeheimbetreiber eine Liste von Wohngeldbeziehern in seinem Pflegeheim zu übermitteln, um die entsprechenden qm-Zahlen beizufügen, scheidet ebenfalls aus. Das wäre gleichzeitig eine Übermittlung von Sozialdaten der Wohngeldbezieher an den Betreiber. Auch hierfür war keinerlei Rechtsgrundlage ersichtlich.
Das angestoßene Verfahren war damit nicht zulässig und widersprach darüber hinaus dem Grundsatz der Erhebung beim Betroffenen. Zulässig gewesen wäre, die Wohngeldbezieher in dem Pflegeheim selbst persönlich anzuschreiben und um Auskünfte zur qm-Zahl der bewohnten Fläche zu bitten. Nach § 67a Abs. 2 SGB X gilt nämlich auch für Sozialdaten der Grundsatz der Datenerhebung beim Betroffenen, sofern keine der dort aufgezählten Gründe vorliegen, die eine Erhebung bei anderen Stellen rechtfertigen. Möglicherweise hätten die Wohngeldbezieher die entsprechenden Angaben bei der Heimleitung erfragen und bestätigen lassen müssen. Allein der geringere Aufwand für die Stadtverwaltung, nur eine Stelle anstatt mehrerer Personen anschreiben zu müssen, rechtfertigt jedoch die zuvor gewählte Vorgehensweise nicht. Die Stadtverwaltung bestätigte, die Hinweise zu den datenschutzrechtlichen Problemen bei der Überprüfung und dem Abgleich der Daten von Wohngeldbeziehern zur Kenntnis genommen zu haben und in der künftigen Arbeit zu berücksichtigen.

Der Amtsermittlungsgrundsatz nach § 20 SGB X umfasst nicht, dass grundsätzlich ohne konkreten Anlass und ohne Differenzierung die Angaben von Dritten verlangt werden können. Sozialdaten sind beim Betroffenen zu erheben, sei denn, es liegt ein in § 67a Abs. 2 SGB X geregelter Ausnahmefall vor.

5.5 Stadt will immer wieder wissen, wie Jugendliche ticken! – Datenschutz bei Jugendstudien

Die Befragung von Kindern und Jugendlichen zur Jenaer Jugendstudie war bereits Gegenstand des 8. Tätigkeitsberichts (13.4) des Thüringer Landesbeauftragten für den Datenschutz (TLfDI) im Berichtszeitraum 2008 bis 2009. Die Jugendstudien werden seit 1997 durchgeführt. Die Kinder und Jugendlichen werden jährlich gebeten, in

einem umfangreichen Fragebogen Auskunft über ihre Lebensbedingungen und den Bedarf an Freizeitangeboten zu geben. Wegen der Ausführlichkeit der Fragen, die erheblich ins Detail gehen und auch die familiäre Situation umfassen, wurde der TLfDI erneut angefragt.
Zur Erinnerung: Schülerbefragungen, die nicht verpflichtend sind, bedürfen der schriftlichen Einwilligung der Sorgeberechtigten und der bereits grundrechtsmündigen Schüler. Diese Einwilligung wird nur dann rechtswirksam erteilt, wenn der Einwilligende die Bedeutung und die Tragweite seiner Entscheidung zu überblicken vermag. Die datenschutzrechtliche Einwilligung ist erforderlich, weil aufgrund der detailreichen Abfrage eine Personenbeziehbarkeit des einzelnen Fragebogens, also ein Rückschluss auf den Auskunft erteilenden Schüler, nicht ausgeschlossen ist. Der Ablauf gestaltete sich im Wesentlichen so, dass der Stadt vom Forschungsinstitut ein Angebot zur Durchführung im jeweiligen Jahr unterbreitet wird. Die Stadt holt sodann die Genehmigung des zuständigen Schulamts ein. Die Schulleitungen werden darauf hingewiesen, dass die Eltern zu informieren sind. Das Forschungsinstitut verteilt eine ausreichende Anzahl an Fragebögen mit Rückumschlägen an die Schulen.
Den Schülern stand es frei, an der Befragung teilzunehmen. Sie konnten sich, ohne dass eine schriftliche Einwilligung der Eltern vorlag, die entsprechenden Fragebögen nehmen und ausfüllen. In die mitgelieferten Umschläge verpackt, wurden sie von den Schülern in eine der vom Forschungsinstitut in der jeweiligen Schule aufgestellten Urne eingeworfen. Nur die Mitarbeiter des Forschungsinstituts verfügten über einen Schlüssel zur Öffnung des Behältnisses. Weder die Schule noch die Stadtverwaltung hatte Zugriff auf die einzelnen Fragebögen. Von den Mitarbeitern des Forschungsinstituts, die auf das Datengeheimnis verpflichtet waren, wurden die Umschläge geöffnet und die Angaben in das automatisierte Statistikprogramm eingegeben. Danach wurden die Fragebögen vernichtet.
Da die Mitarbeiter des Forschungsinstituts keine Kenntnis darüber haben, wer von den Schülern aus einer Schule letztendlich die Fragebögen ausgefüllt hat, kann die Anonymität gewährleistet werden. Die statistisch aufbereiteten Daten, die veröffentlicht werden, erlauben nach den Darlegungen des Forschungsinstituts auch dann, wenn nur wenig Schüler einer Schule teilgenommen haben, keinen direkten Rückschluss auf den Einzelnen. Die dem TLfDI gegenüber geäußerten Befürchtungen und Bedenken hinsichtlich der Reanonymi-

sierbarkeit des veröffentlichten Ergebnisses der Forschungsarbeit auf einzelne Schüler konnten damit ausgeräumt werden.
Handlungsbedarf stellte der TLfDI jedoch in zwei Punkten fest:
Offenbar gab es zuletzt Defizite bei der Information der Eltern. Dies könnte darauf zurückzuführen sein, dass aufgrund der alljährlichen Befragung eine „Gewohnheit“ eingetreten ist und dadurch den Informationen nicht mehr das gebotene Gewicht beigemessen wurde. Um dies wiederherzustellen, wurde zugesagt, dass zukünftig jedem Schüler, der an der Befragung teilnehmen kann, eine Einwilligungserklärung mitgegeben wird. Nur wenn eine unterschriebene Einwilligung zurückgegeben wird, können die Fragebögen ausgehändigt werden. Selbstverständlich dürfen die Einwilligungserklärungen nicht mit den Fragebögen zusammengeführt werden, weil damit die Anonymisierung wieder aufgehoben wäre.
Außerdem gab es in den geprüften schriftlichen Unterlagen zur Auftragserteilung der aktuellen Jugendstudie keine zusammenhängende Darstellung des konkreten Ablaufs. Der Ablauf musste verschiedenen Dokumenten, die in dem Zusammenhang erstellt worden waren, entnommen werden. Zukünftig werden jedoch die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Angaben hinsichtlich des Ablaufs in das Angebot des Forschungsinstituts aufgenommen.
Insgesamt haben sich auch bei der aktuellen Studie keine Hinweise darauf ergeben, dass eine Reanonymisierung und damit ein Bezug auf einen einzelnen Schüler aufgrund der Darstellung des Ergebnisses der Jugendstudie möglich ist. Keine der beteiligten Stellen hat Kenntnis darüber, welcher Schüler tatsächlich teilgenommen hat. Weiterhin haben sich keine Hinweise darauf ergeben, dass die dargelegten technischen und organisatorischen Maßnahmen zum Schutz der Angaben der Schüler nicht eingehalten worden wären, obwohl diese nicht zusammenhängend, also als Checkliste, vorlagen.
Zwischenzeitlich hat sich zumindest eine weitere Kommune zur Durchführung von Jugendstudien entschieden, andere Kommunen haben ebenfalls Interesse daran bekundet.

Auch wenn in einer Schule bereits mehrere Studien durchgeführt wurden, kann man nicht davon ausgehen, dass der Ablauf allgemein bekannt ist und alle damit einverstanden sind. Auf die Einwilligungen der Eltern und der bereits grundrechtsmündigen Schüler kann nicht verzichtet werden.

5.6 Karnevalswagen als Beweis unrechtmäßiger Datenübermittlung?

Ein ehemaliger Bediensteter einer Gemeinde wandte sich wegen einer Fülle von datenschutzrechtlichen Unzulänglichkeiten in seiner Gemeinde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Ausgangspunkt war, dass sich ein Gemeinderatsmitglied berufen sah, dem Beschwerdeführer nachzuweisen, dass er sich am Eigentum der Gemeinde vergriff und sich mit der Kamera auf die Lauer legte. Dabei angefertigte Fotos legte das Gemeinderatsmitglied dem Bürgermeister als Dienstherrn vor. Das Beschäftigungsverhältnis zwischen der Gemeinde und dem Bediensteten wurde letztendlich durch Vergleich beendet, Verfehlungen bildeten nicht den Grund hierfür. Leider ist der Vorgang publik geworden, die vermeintlichen Verfehlungen wurden sogar im Karnevalsumzug der Gemeinde dargestellt. Der Beschwerdeführer vermutete nun, dass es ein „abgekartetes Spiel“ war und die Darstellung auf dem Umzugswagen durch die Gemeinde, vertreten durch den Bürgermeister, lanciert worden sei.
Auf Nachfrage erklärte der Bürgermeister, das Gemeinderatsmitglied sei nicht durch ihn oder die Gemeinde mit der Beweiserhebung beauftragt gewesen. Wenn ihm jedoch eine Verfehlung durch Dritte bekannt gegeben wird, müsse er dem nachgehen. Eine Information an Außenstehende oder an die Öffentlichkeit habe es durch die Gemeinde aber zu keinem Zeitpunkt gegeben. Wie das in einer kleineren Gemeinde so sei, könnten durchaus sowohl der Beschwerdeführer als auch seine Familienmitglieder Dritten gegenüber die Angelegenheit angesprochen haben.
Damit stand in diesem Fall Aussage gegen Aussage. Weder aus den Angaben des Beschwerdeführers noch aus den Angaben des Bürgermeisters konnten konkrete Anhaltspunkte für berechtigte Zweifel an der Richtigkeit des Vorbringens des jeweils anderen entnommen werden. Die Prüfmöglichkeit des Sachverhalts durch den TLfDI war in diesem Zusammenhang an ihre Grenzen geraten. Dem TLfDI stehen als Kontrollbehörde für öffentliche Stellen keine besser geeigneten Mittel zur Verfügung, die Angaben des Bürgermeisters weiter zu überprüfen. Dem TLfDI ist es nicht möglich, in Wahrnehmung seiner Kontrollkompetenz im öffentlichen Bereich, etwa wie in einem Strafverfahren, Zeugenvernehmungen und Beschlagnahmen

durchzuführen. Die öffentlichen Stellen des Landes haben zwar die Pflicht, auf alle Fragen des TLfDI im Zusammenhang mit einer Kontrolle wahrheitsgemäß und umfassend zu antworten und Zugang zu Dokumenten zu gewähren (§ 38 Thüringer Datenschutzgesetz [ThürDSG]). Ob sie diesen Pflichten ordnungsgemäß nachkommen, kann der TLfDI leider nicht immer zweifelsfrei überprüfen. Im vorliegenden Fall war daher nicht auszuschließen, dass eine Datenübermittlung durch die Gemeinde an die Öffentlichkeit vorlag, doch bedurfte es zum Nachweis dafür konkreter belastbarer Tatsachen. Solche waren indes nicht vorhanden.
Die weiteren Hinweise des Beschwerdeführers, dass in der Gemeinde keine schriftlichen Festlegungen zur Einhaltung der datenschutzrechtlichen Vorgaben vorhanden waren, griff der TLfDI selbstverständlich auf. Er forderte die Gemeinde auf, Dienstanweisungen und weitere Festlegungen zu den technischen organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten zu treffen bzw. solche schriftlich niederzulegen. Da dies im Regelfall nicht von heute auf morgen bewerkstelligt werden kann, ist dieser Fall beim TLfDI leider noch nicht abgeschlossen.

Nicht immer reichen die Mittel des TLfDI aus, das Vorbringen eines Beschwerdeführers zu datenschutzrechtlichen Mängeln in allen Einzelheiten zu überprüfen. Öffentliche Stellen sind verpflichtet, wahrheitsgemäß auf die Fragen des TLfDI zu antworten und Zugang zu allen Unterlagen, die mit der datenschutzrechtlichen Kontrolle im Zusammenhang stehen, zu gewähren. Steht Aussage gegen Aussage, bedarf es konkreter Anhaltspunkte für Zweifel an der Richtigkeit einer Aussage. Bestehen solche Zweifel nicht, wird es für den TLfDI schwierig, einen datenschutzrechtlichen Verstoß nachzuweisen.

5.7 Bevor „das Kind in den Brunnen fällt“: besser vom TLfDI beraten lassen!

Die Stadtverwaltung Arnstadt bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beurteilung des Verfahrens und der Datenschutzhinweise zu einer Bürgerbefragung über die Neugestaltung des dortigen Marktplatzes.
Danach wollte die Stadtverwaltung die Fragebögen an alle Bürger der Stadt ab vollendetem 14. Lebensjahr versenden, wobei sie die Adressdaten aus dem Einwohnerverzeichnis nutzen wollte. Für den

Ausdruck und Versand der Fragebögen beabsichtigte die Stadtverwaltung Arnstadt, das Thüringer Landesrechenzentrum mittels einer Vereinbarung zur Datenverarbeitung im Auftrag nach § 8 Thüringer Datenschutzgesetz (ThürDSG) zu beauftragen. Weiterhin sicherte die Stadtverwaltung zu, innerhalb ihrer Behörde die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes einzuhalten. Laut der Datenschutzhinweise sollten die personenbezogenen Daten der Bürger ausschließlich für die Einwohnerbefragung verwendet werden. Eine Weitergabe der personenbezogenen Daten an Dritte schloss die Stadtverwaltung ausdrücklich aus und sicherte zugleich zu, spätestens drei Monate nach Ende der Einwohnerbefragung diese Daten zu löschen. Zugleich räumte die Stadtverwaltung den Bürgern das Recht auf Auskunft, Berichtigung und Löschung ihrer gespeicherten personenbezogenen Daten ein. Mit seiner Unterschrift hatte der Bürger die Möglichkeit, zu bestätigen, dass er freiwillig in die Datenerhebung, Datenverarbeitung und Nutzung zum vorgenannten Zweck eingewilligt hat. Der TLfDI teilte der Stadtverwaltung Arnstadt nach Prüfung der Unterlagen abschließend mit, dass der beabsichtigte Verfahrensweg und die Datenschutzhinweise den datenschutzrechtlichen Bestimmungen entsprechen.

Kommunen, die sich vor Beginn komplexer Vorhaben, wie z. B. einer Bürgerbefragung, vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit beraten lassen, können sich damit unter Umständen eine Menge Ärger und Arbeit ersparen.

5.8 Datenerhebung mittels Mülltonne? – Aufkleber mit personenbezogenen Daten

Bereits in seinem achten Tätigkeitsbericht (Nr. 5.16 – Datenhunger der Abfallwirtschaftsgesellschaft Gotha, S. 56 f.) hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über Datenschutzprobleme bei Kommunalen Abfallentsorgungsunternehmen berichtet.
Im Berichtszeitraum erfuhr der TLfDI nunmehr, dass im Versorgungsgebiet des Abfallwirtschaftsbetriebs des Landkreise Saale-Holzland (AWB) an den Tonnen für Papiermüll Aufkleber angebracht waren, auf denen die Kunden des AWB Straßenname, Hausnummer, Postleitzahl und Ort des Abfalltonnenstandorts anzugeben

hätten. Der TLfDI schaltete sich umgehend ein und forderte den AWB zur Stellungnahme auf.
Der AWB vertrat zunächst die unzutreffende Auffassung, dass es sich bei diesen Daten nicht um personenbezogene, sondern lediglich um anonymisierte Daten handele. Dies veranlasste den TLfDI zu folgender rechtlicher Klarstellung:
Nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sind personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Anonymisieren ist gemäß § 3 Abs. 9 ThürDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Da ein objektiver Dritter ohne größeren Aufwand von den o. g. Daten auf die anschluss- und benutzungspflichtigen natürlichen Personen schließen konnte, handelte es sich bei diesen Daten zweifellos um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG.
Wie der AWB weiterhin vortrug, sei es fraglich, ob es sich bei den Grundstücksangaben an den Müllbehältern um personenbezogene Daten handele, da sich der Eigentümer des anschlusspflichtigen Grundstückes nur mit größerem Aufwand – hier durch Anfrage beim Amtsgericht / Grundbuchamt – ermitteln lasse.
Hierzu führte der TLfDI aus, dass im Regelfall zwar die Kenntnis der Grundbucheintragung zur Bestimmung des anschluss- und benutzungspflichtigen Eigentümers erforderlich sei. Jedoch sei die Beschaffung des nötigen Zusatzwissens durch eine Anfrage im Grundbuchamt nicht mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft im Sinne von § 3 Abs. 9 ThürDSG verbunden. Diese Beurteilung entspricht der datenschutzrechtlichen Kommentarliteratur. Die Richtlinie 95/46/EG (nachfolgend: Datenschutzrichtlinie) bezieht in die Definition der personenbezogenen Daten (Art. 2 lit. a) „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“ ein und definiert als bestimmbar eine Person, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung einer Kennnummer …“. Nach Erwägungsgrund 26 der Datenschutzrichtlinie sollen für die Bestimmbarkeit „alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen oder von einem Dritten eingesetzt

werden können, um die betreffende Person zu bestimmen.“ Zu diesen Mitteln gehört sowohl vorhandenes als auch mit nicht unverhältnismäßigem Aufwand beschaffbares Zusatzwissen. Hierfür genügt es, dass ein nötiges Zusatzwissen zugänglich ist. Ob sich der Recherchierende dieses Zusatzwissen erst besorgen muss und ob seine entsprechende Absicht dafür besteht, spielt keine Rolle. So sind z. B. die mit einem Kfz-Kennzeichen verbundenen Daten als personenbezogen anzusehen, obwohl deren Erschleichen durch falsche Angaben ordnungswidrig ist. Diese Wertung muss daher erst recht für Eigentümer von Grundstücken gelten, die in einem (keine Person aufweisenden) Datensystem dargestellt, beschrieben oder abgebildet sind, da sie ganz überwiegend von jedermann unschwer ermittelt werden können. (Simitis, Bundesdatenschutzgesetz-Kommentar, 8. Auflage, Anm. 24, 26, 28, 31 und 57 zu § 3, S. 330 ff.).

Nach § 4 Abs. 1 ThürDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder angeordnet oder soweit der Betroffene eingewilligt hat. Um eine solche „andere Rechtsvorschrift“ im Sinne von § 4 Abs. 1 ThürDSG handelt es sich bei § 30 Abs. 2 Satz 1 des Thüringer Gesetzes über die Vermeidung, Verminderung, Verwertung und Beseitigung von Abfällen (ThürAbfG). § 30 Abs. 2 Satz 1 ThürAbfG berechtigt die öffentlich-rechtlichen Entsorgungsträger, die zu ihrer Aufgabenerfüllung erforderlichen personenbezogenen Daten zu erheben, wobei sie verpflichtet sind, mittels Satzung zu regeln, bei welchen Personen oder Stellen welche personenbezogenen Daten erhoben werden sollen.

Die Recherchen des TLfDI ergaben jedoch, dass die Satzung über die Vermeidung, Verwertung und Entsorgung von Siedlungsabfällen (AbfWS) des Saale-Holzland-Kreises eine solche Regelung nicht enthielt. Entgegen der Auffassung des AWB ist auch § 5 AbfWS, der die Anschluss- und Benutzungspflichtigen lediglich zur Abfalltrennung verpflichtet, nicht als eine Regelung gemäß § 30 Abs. 2 anzusehen. An der fehlenden Rechtsgrundlage hätte auch die Umsetzung der Absicht des ABW nichts geändert, eine Regelung in die AbfWS einzufügen, wonach bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Bestimmungen des § 30 ThürAbfG und des ThürDSG gelten sollen. Denn eine solche Regelung wäre in jedem Fall zu unbestimmt im Sinne von § 30 Abs. 2 Satz 2 ThAbfG gewesen, weil sie gerade nicht bestimmt, bei welchen Personen oder Stellen welche personenbezogenen Daten zu erheben sind.

Daher stellte der TLfDI im Ergebnis fest, dass der AWB bei der Entsorgung von Papiermüll personenbezogene Daten erhoben hat. Mangels einer geeigneten Rechtsgrundlage im Sinne von § 30 Abs. 2 ThürAbfG handelte es sich hierbei um einen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 4 Abs. 1 ThürDSG, in Form einer unzulässigen Datenerhebung.
Letztendlich erklärte der AWB, dass er die AbfWS umgehend um eine Erlaubnisnorm zur Erhebung der personenbezogenen Daten der Postleitzahl, des Ortes, des Straßennamen und der Hausnummer des betreffenden Grundstückes ergänzen werde. Die Erhebung dieser Daten diene, so der AwB, zum einen dem Dienstleistungsbetrieb der Überwachung und Durchsetzung des Anschluss- und Benutzungszwanges in der Abfallfraktion Papier/Pappe/Kartonagen und zum anderen einer näherungsweisen Überwachung der entsorgten Abfallmenge.
Durch eine solche Ergänzung der AbfWS trägt der AWB der Forderung des § 30 Abs. 2 Satz 2 ThAbfG Rechnung, wonach öffentlich-rechtliche Entsorgungsträger berechtigt sind, die zu ihrer Aufgabenerfüllung erforderlichen personenbezogenen Daten zu erheben.

Insbesondere im Abfall- und Entsorgungswesen bestehen nach Erfahrungen des TLfDI immer wieder Unklarheiten zu den datenschutzrechtlichen Pflichten kommunaler Entsorgungsunternehmen. Die hier agierenden öffentlich-rechtlichen Entsorgungsträger sind verpflichtet, mittels Satzung zu regeln, bei welchen Personen oder Stellen welche personenbezogenen Daten konkret erhoben werden.

5.9 Schatten der Vergangenheit – „Ex-Stasi“ im Stadtrat durch den TLfDI „outen“?

Eine Stadtverwaltung teilte dem Thüringer Landesbeauftragen für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass der dortige Stadtrat die Überprüfung seiner Mitglieder gemäß §§ 19, 20 und 21 Stasi-Unterlagen-Gesetz beschlossen habe. Nachdem die zuständige Kommunalaufsicht nicht die Aufsicht über das hierzu erforderliche Verfahren übernehmen wollte, sollte der TLfDI die „fachliche Aufsicht und Leitung des Überprüfungsverfahrens übernehmen, begleiten bzw. beratend tätig …“ werden.
Der TLfDI teilte der Stadtverwaltung hierzu mit, dass die fachliche Aufsicht und Leitung bzw. Begleitung eines Überprüfungsverfahrens

gemäß Stasi-Unterlagen-Gesetz außerhalb seines Kompetenzbereichs liege. Dies ergibt sich insbesondere aus den Regelungen zu den Aufgaben des TLfDI aus §§ 37 bis 40 ThürDSG und den Rechten des Betroffenen in den §§ 5 und 11 bis 17 Thüringer Datenschutzgesetz (ThürDSG). Der TLfDI empfahl, sich in dieser Angelegenheit ggf. an den Landesbeauftragten des Freistaates Thüringen zur Aufarbeitung der SED-Diktatur zu wenden.
Zugleich wies der TLfDI auf den sorgsamen Umgang mit den bei der Überprüfung ggf. zu erwartenden hochsensiblen personenbezogenen Daten im Sinne von § 4 Abs. 5 ThürDSG hin. Über den weiteren Fortgang dieses Falls erhielt der TLfDI mangels Zuständigkeit keine weiteren Informationen – was datenschutzrechtlich korrekt ist.

Über die Aufgaben und Zuständigkeiten des TLfDI besteht auf kommunaler Ebene noch deutlicher Informationsbedarf. Für eine Überprüfung von Stadtratsmitgliedern nach dem Stasi-Unterlagen-Gesetz ist der TLfDI nicht zuständig.
Die erforderlichen datenschutzrechtlichen Kenntnisse im Freistaat Thüringen und in seinen Kommunen zu vermitteln, bleibt daher eine Aufgabe des TLfDI, die einen langen Atem erfordert.

5.10 „Werbepost“ vom Oberbürgermeister – leider ohne Rechtsgrundlage und Einwilligung!

Im Berichtszeitraum ging dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Vielzahl von Schreiben von Bürgern der Stadt Jena zu, die sich gleichlautend darüber beschwerten, dass mit ihren im Rahmen einer Unterschriftensammlung für ein Moratorium erhobenen und an den Oberbürgermeister übergebenen Daten nach ihrer Meinung nicht datenschutzkonform umgegangen worden sei.
Die Beschwerdeführer informierten den TLfDI darüber, dass Ende des Jahres 2013 ca. 10.000 Unterschriften für ein Moratorium zur Bebauung eines städtischen Platzes an den Oberbürgermeister übergeben worden seien. Die Unterschriften seien von einer Bürgerinitiative freiwillig gesammelt worden. Die Bürgerinnen und Bürger, die ein solches Moratorium unterstützten, hätten sich jeweils mit ihren Nachnamen, ihren Vornamen, ihren Adressen, dem Datum und ihren Unterschriften in der Unterschriftensammlung eingetragen. Nicht zuletzt aufgrund der zahlreichen Unterstützer der Unterschriften-

sammlung fasste der Stadtrat Ende Januar 2014 einen Beschluss, dass eine Bürgerbefragung per Post zur Bebauung des Platzes stattfinden sollte. Diese Bürgerbefragung führte die Stadt sodann durch. Entsprechend den Informationen der Stadtverwaltung wurden dafür die Daten aus der vorangegangenen Unterschriftensammlung von Verwaltungsmitarbeitern ausgewertet (verarbeitet), nach Nebenwohnsitz/Hauptwohnsitz sowie Alter (älter als 16 Jahre) der Unterschriftsleistenden selektiert und für ein persönliches Anschreiben des Oberbürgermeisters an die Unterzeichner der Unterschriftensammlung genutzt.

Zur Klärung und datenschutzrechtlichen Bewertung der Angelegenheit kontrollierte der TLfDI die Stadtverwaltung gemäß § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) vor Ort.

Im Ergebnis stellte der TLfDI Folgendes fest:

Die Verarbeitung und Nutzung von personenbezogenen Daten der Unterschriftensammlung zum Moratorium für persönliche Anschreiben des Oberbürgermeisters war unzulässig. Dies ergab sich aus § 4 Abs. 1 Satz 1 ThürDSG, weil im zu beurteilenden Sachverhalt weder ein Gesetz oder eine andere Rechtsvorschrift die Verarbeitung und Nutzung der genannten personenbezogenen Daten erlaubte oder anordnete, noch eine Einwilligung der betroffenen Bürger, die sich im Rahmen der Unterschriftensammlung mit ihren personenbezogenen Daten eingetragen hatten, vorlag.

§ 15 Abs. 1 Thüringer Kommunalordnung (ThürKO) kam hier als Rechtsgrundlage für die Verarbeitung und Nutzung der personenbezogenen Daten der Unterschriftleistenden auf den Listen des Moratoriums nicht in Betracht. Zwar lag die dafür erforderliche wichtige Gemeindeangelegenheit mit der Frage der Bebauung des städtischen Platzes nach Auffassung des TLfDI im konkreten Fall vor. Im Ergebnis kam § 15 Abs. 1 ThürKO hier aber nicht als Rechtsgrundlage für die Datenerhebung infrage, weil danach alle Einwohner über die wichtige Gemeindeangelegenheit zu unterrichten gewesen wären. Im vorliegenden Fall hatte der Oberbürgermeister aber nur die Unterzeichner der Unterschriftensammlung, die das Moratorium befürworteten, angeschrieben und somit nur deren Daten verarbeitet.

§ 29 Abs. 2 Nr. 1 ThürKO schied nach Auffassung des TLfDI ebenfalls als Rechtsgrundlage für die Nutzung von Adressdaten jener Bürger aus, die in der Unterschriftensammlung für das Moratorium unterschrieben hatten. Denn in der Sache ging es hier ja – wie bereits gesagt – um eine wichtige Gemeindeangelegenheit im Sinne von

§ 15 Abs. 1 ThürKO. § 29 Abs. 2 Nr. 1 ThürKO, der nur die laufenden Angelegenheiten des eigenen Wirkungskreises erfasst, die keine grundsätzliche Bedeutung haben, war demzufolge nicht anwendbar.
Ferner konnte auch § 34 Abs. 4 Thüringer Meldegesetz (ThürMeldeG) nicht als Rechtsgrundlage für eine Verarbeitung und Nutzung personenbezogener Daten durch die Stadt aus den genannten Unterschriftensammlungen herangezogen werden. Dies ergab sich daraus, dass eine anzustellende Interessenabwägung im konkreten Fall zugunsten des Schutzes des Rechts auf informationelle Selbstbestimmung aller Unterzeichner der Unterschriftensammlung ausfiel, weil die Verarbeitung ihrer personenbezogenen Daten durch den Oberbürgermeister in Form eines Anschreibens an die Gegner der Bebauung des städtischen Platzes hier nicht erforderlich war. Denn der Oberbürgermeister konnte hier ebenso gut mittels einer Abstimmungsbroschüre noch einmal die Vorteile einer Bebauung des Platzes deutlich machen.
Das Speichern oder Nutzen dieser personenbezogenen Daten konnte auch nicht nach § 20 Abs. 2 ThürDSG gerechtfertigt werden, da im vorliegenden Sachverhalt kein Grund ersichtlich war, der eine Zweckänderung für die Nutzung der personenbezogenen Daten rechtfertigte.
Schließlich war im konkreten Fall auch keine Einwilligung der Betroffenen im Sinne von § 4 Abs. 1 Satz 1 ThürDSG in die Verarbeitung und Nutzung der personenbezogenen Daten zu erkennen. Dies ergab sich daraus, dass die Unterzeichner der genannten Unterschriftensammlung an keiner Stelle signalisiert hatten, dass sie mit einer weiteren Korrespondenz gegenüber der Stadt in der Angelegenheit rechneten, geschweige denn einverstanden wären. Auch bei der Übergabe der Unterschriftlisten war eine solche weitere Dialogbereitschaft von keinem Beteiligten signalisiert oder später behauptet worden.
Der TLfDI hat im Ergebnis der datenschutzrechtlichen Kontrolle und Prüfung die somit ohne Rechtsgrundlage erfolgte Verarbeitung und Nutzung von Unterschriften der Unterschriftensammlung für persönliche Anschreiben des Oberbürgermeisters an die Unterschriftsleistenden als datenschutzrechtliche Verletzung gemäß § 39 Abs. 1 ThürDSG beanstandet und die zuständige Aufsichtsbehörde informiert.
Die im Sinne des Datenschutzes rechtswidrige Maßnahme war aber bereits durchgeführt und abgeschlossen, sodass die Behebung dieser

datenschutzrechtlichen Verletzung i. S. d. § 39 Abs. 1 Satz 1 ThürDSG nicht mehr möglich war. Der TLfDI forderte die Stadtverwaltung daher auf, für die Zukunft darauf hinzuwirken, dass vorgenannte datenschutzrechtliche Verstöße verhindert werden.
Abschließend teilte die Stadtverwaltung auf Nachfrage des TLfDI mit, dass jegliche im Zusammenhang mit der Unterschriftensammlung gespeicherten Daten gelöscht worden seien.

Gut gemeint ist nicht immer gut gemacht: Die Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 Satz 1 ThürDSG nur zulässig, wenn das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Dies gilt selbst in dem Fall, dass ein Oberbürgermeister die personenbezogenen Daten nutzen will, um mit seinen Einwohnern in einen Dialog zu treten. Im Falle der Einwilligung ist die Verarbeitung oder Nutzung personenbezogener Daten gemäß § 4 Abs. 1 Satz 2 ThürDSG nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist. Bei Bürgerbefragungen oder Unterschriftensammlungen haben die Bürger dabei ihre Einwilligung zu erteilen, dass sie mit der Verarbeitung und Nutzung ihrer personenbezogenen Daten für einen konkret festzulegenden Zweck einverstanden sind. Für Bürgeranträge, Volksbegehren und Volksentscheide auf Landesebene ist dies in §§ 5 und 6 Abs. 1 Satz 3 Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG) geregelt.

5.11 Keine Meldedaten für den Großvater: nicht lustig, aber datenschutzkonform

Ein Bürger hatte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum gebeten, ihm bei der Suche nach dem derzeitigen Aufenthalts- und Wohnort seiner Tochter und seiner Enkeltochter zu helfen. Ferner begehrte der Bürger Hilfe bei der Beseitigung einer für ihn bestehenden Auskunftssperre zu seiner Tochter im Melderegister. Er sei ein untadeliger Rentner und habe Veranlassung, anzunehmen, dass beim TLfDI ganz böswillige Falschmeldungen über ihn eingegangen seien. Seine Tochter sei verzogen und habe mit der Sperre erreicht, dass er sie und sein Enkelkind nicht mehr erreichen könne.

Ausweislich der vom Beschwerdeführer vorgelegten Schreiben hatte er sich an das Meldeamt mit der Bitte um Melderegisterauskunft hinsichtlich der jetzigen Anschrift seiner Tochter gewandt. Diesem Auskunftsersuchen entsprach das Meldeamt nicht, vielmehr forderte es den Beschwerdeführer zur Begründung eines berechtigten/rechtlichen Interesses an der Auskunft auf.
Die zuständige Meldebehörde informierte den TLfDI auf dessen Bitte dahingehend, dass die Tochter des Beschwerdeführers einen Antrag auf Einrichtung einer Auskunftssperre gemäß § 31 Abs. 7 Thüringer Meldegesetz (ThürMeldeG) gestellt hatte. Als Gründe habe die Tochter große Probleme im Umgang mit dem Beschwerdeführer, ihrem Vater, angegeben. Diese zögen sich bereits über mehrere Jahre hin, die Aggressivität seitens des Vaters habe zugenommen. Es standen Beschimpfungen und Beleidigungen in verbaler und schriftlicher Form im Raum. Dies habe die Tochter mit verschiedenen Schreiben des Beschwerdeführers belegt. Die Tochter habe sich deshalb zu einem Umzug entschlossen. Die Auskunftssperre sei antragsgemäß im Melderegister eingetragen worden. Auf das schriftliche Auskunftsersuchen des Beschwerdeführers hin wurde die Tochter gemäß § 31 Abs. 7 Satz 2 ThürMeldeG angehört. In Folge erhielt der Beschwerdeführer eine schriftliche Mitteilung vom Meldeamt, dass es eine Auskunft zu seiner Tochter wegen einer eingetragenen Melderegisterauskunftssperre nicht erteilen könne. Das Meldeamt habe den Beschwerdeführer vielmehr aufgefordert, ggf. sein rechtliches bzw. berechtigtes Interesse an der Auskunft nachzuweisen. Das habe er nicht getan.
Der TLfDI hat den Beschwerdeführer im Ergebnis darüber informiert, dass die Verweigerung der Melderegisterauskunft an ihn wegen der für seine Tochter eingetragenen Melderegisterauskunftssperre und seinem nicht vorgetragenen rechtlichen Interesse an dieser Auskunft nicht nur datenschutzrechtlich unbedenklich, sondern datenschutzrechtlich erforderlich war (§ 31 Abs. 7 Satz 2 ThürMeldeG). Weiter hat der TLfDI dem Beschwerdeführer mitgeteilt, dass eine eingetragene Auskunftssperre nicht zwingend zu einer Verweigerung jedweder Melderegisterauskunft führt. Hat die anfragende Person gegenüber der Meldebehörde ein berechtigtes Interesse an der Erteilung der Meldedaten glaubhaft gemacht – dies ist in der Regel anzunehmen, wenn z. B. der Auskunftssuchende die erbetenen Daten zur Rechtsverfolgung/Rechtsverteidigung benötigt –, gilt die Auskunftssperre ggf. nicht in vollem Umfang. Ob allerdings die Voraus-

setzungen der für die Tochter eingetragenen Melderegisterauskunftssperre im konkreten Fall vorlagen, hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit mangels Zuständigkeit nicht zu prüfen. Diese Aufgabe liegt allein im Kompetenzbereich der zuständigen Meldebehörde. Der TLfDI hat den Beschwerdeführer ergänzend darüber informiert, dass die Ablehnung seines Auskunftsersuchens durch die Meldebehörde für ihn einen (belastenden) Verwaltungsakt im Sinne von § 35 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) darstelle und diese Ablehnung seinerseits mit einem Widerspruch gemäß §§ 68 ff. Verwaltungsgerichtsordnung (VwGO) und einer Klage (§ 42 Abs. 1 VwGO) angefochten werden könne.
Schließlich ist auf Folgendes hinzuweisen: Zum 1. November 2015 ist das Bundesmeldegesetz (BMG) in Kraft getreten. Das Meldewesen liegt nunmehr in der ausschließlichen Gesetzgebungskompetenz des Bundes. Die Regelungen zu Auskunftssperren im Melderegister sind aber im Wesentlichen nicht verändert worden (vgl. § 51 BMG).

Eine Auskunftssperre hat die Meldebehörde gemäß § 51 Abs. 1 BMG auf Antrag oder von Amts wegen im Melderegister einzutragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Die Prüfung, ob die Voraussetzungen hierfür im Einzelfall vorliegen, ist dem TLfDI versagt. Er kann lediglich Hilfe bei der Aufklärung leisten, warum und aus welchen Gründen dem Bürger eine Auskunft aus dem Melderegister versagt wird.

5.12 Aushändigung einer Meldebescheinigung an Nichtberechtigte

Ein Beschwerdeführer stellte im Berichtszeitraum dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) per E-Mail die Kopie einer Meldebescheinigung (hinsichtlich seiner Person) zur Verfügung. Seine Mutter habe diese vom Meldeamt der Stadtverwaltung Schmalkalden erhalten und ihm zur Kenntnis vorgelegt. Sie beabsichtigte, diese Meldebescheinigung in einem Gerichtsprozess gegen ihn zu verwenden. Der Beschwerdeführer habe daraufhin in der Stadtverwaltung angerufen, um zu

klären, ob seine Mutter oder ggf. eine dritte Person diese Meldebescheinigung angefordert habe und ob ein berechtigtes Interesse vorgetragen worden sei. Der Beschwerdeführer ging davon aus, dass die Meldebescheinigung entgegen aller Datenschutzbestimmungen an einen Nichtberechtigten ausgehändigt wurde, sodass er den TLfDI um Datenschutz-Hilfe bat.
Der TLfDI wandte sich an die Stadtverwaltung Schmalkalden mit der Bitte um Stellungnahme zur Angelegenheit, insbesondere um Mitteilung der Rechtsgrundlage für die ggf. erfolgte Übermittlung der personenbezogenen Daten des Beschwerdeführers an seine Mutter oder sonstige Dritte.
Der TLfDI teilte dem Beschwerdeführer nach Eingang der Stellungnahme der Stadtverwaltung und datenschutzrechtlicher Prüfung der Angelegenheit mit, dass die Mutter des Beschwerdeführers gegenüber der Meldebehörde ein berechtigtes Interesse an der Erteilung der Meldedaten glaubhaft gemacht habe und ihr die Meldebescheinigung deshalb zur Verfügung gestellt worden sei. Das Vorliegen eines berechtigten Interesses ist in der Regel dann anzunehmen, wenn der Auskunftssuchende die erbetenen Daten zur Rechtsverfolgung/Rechtsverteidigung benötigt. Hier handelt es sich zudem um ein rechtliches Interesse, das als Kriterium insbesondere zur Durchsetzung von Rechtsansprüchen gilt (vgl. dazu Medert/Süßmuth, Melderecht des Bundes und der Länder, Kommentar, Teil I: Bundesrecht, I C Erl. § 21 MRRG, Rz. 31). Das berechtigte Interesse wurde dem TLfDI seitens der Stadtverwaltung Schmalkalden dargelegt. Auskunftssperren im Datensatz des Beschwerdeführers lagen nach Angaben der Stadtverwaltung nicht vor.
Der TLfDI hat den Beschwerdeführer im Ergebnis darüber informiert, dass die in Rede stehende Auskunftserteilung gemäß § 21 Melderechtsrahmengesetz i. V. m. § 31 Abs. 4 Thüringer Meldegesetz datenschutzrechtlich zulässig gewesen ist.
Eine ausführliche datenschutzrechtliche Bewertung der Angelegenheit hat der TLfDI dem Beschwerdeführer bisher nicht zur Verfügung gestellt. Dies geschah aus folgenden Gründen nicht: Die Bewertung der Stadtverwaltung Schmalkalden beinhaltete zum einen sehr sensible Daten zur Person des Beschwerdeführers. Zum anderen hatte sich der Beschwerdeführer ausschließlich per E-Mail an den TLfDI gewandt. Um eine sichere Übermittlung sensibler personenbezogener Daten gewährleisten zu können, bat der TLfDI den Beschwerdeführer um Übersendung seines öffentlichen Schlüssels für

eine verschlüsselte Übersendung der genannten Daten per E-Mail oder um Mitteilung seiner postalischen Anschrift. Leider antwortete der Beschwerdeführer bisher nicht auf diese Bitte des TLfDI.
Zum 1. November 2015 ist das Bundesmeldegesetz (BMG) in Kraft getreten. Das Meldewesen liegt nunmehr in der ausschließlichen Gesetzgebungskompetenz des Bundes. Es ist aber dabei geblieben, dass bei Glaubhaftmachung eines berechtigten Interesses eine erweiterte Melderegisterauskunft erteilt werden darf (§ 45 BMG).

Das Melderegister ist kein Buch mit „sieben Siegeln“, soll aber zum Schutz personenbezogener Daten von Betroffenen auch nicht für jedermann im Detail zur Verfügung stehen. Bei berechtigtem Interesse (z. B. zur Durchsetzung von Rechtsansprüchen) darf die Meldebehörde aber eine erweiterte Melderegisterauskunft erteilen.

5.13 Besonderer Meldeschein: Bayerisches Muster vom TLfDI abgelehnt

Aufgrund einer Bürgeranfrage und im Zuge der Reform des Meldewesens wollte eine Stadt in Thüringen den zur Abrechnung des Kurbeitrages genutzten besonderen Meldeschein für Beherbergungsbetriebe (§ 30 Bundesmeldegesetz (BMG)) neu und vor allem auch datenschutzgerecht gestalten. Die Stadt wandte sich deshalb im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Prüfung ihres – nach Angaben der Stadt ursprünglich aus einer bayerischen Gemeinde stammenden – Meldescheinentwurfs.
Gemäß § 30 Abs. 1 BMG haben die Leiter der Beherbergungsstätte besondere Meldescheine bereitzuhalten und darauf hinzuwirken, dass die betroffenen Personen (die Beherbergten) ihrer Meldepflicht nachkommen. Die Meldescheine enthalten vom Grundsatz die in § 30 Abs. 2 BMG aufgeführten Daten. Gemäß § 30 Abs. 3 BMG i. V. m. § 9 Thüringer Kommunalabgabengesetz dürfen Gemeinden durch Satzung zusätzlich zu diesen in § 30 Abs. 2 des BMG genannten Daten weitere für die Erhebung des Kurbeitrags erforderliche Daten auf dem Meldeschein erheben.

Der TLfDI musste nach datenschutzrechtlicher Prüfung des ihm im Entwurfsstadium vorgelegten besonderen Meldescheines mehrere Punkte kritisch anmerken:

Zunächst war auf dem vorgelegten Entwurf des Meldescheines das „Geburtsdatum des begleitenden Ehegatten/Lebenspartners“ anzugeben. Gemäß § 29 Abs. 2 BMG sind aber mitreisende Angehörige auf dem Meldeschein nur der Zahl nach anzugeben. Zwar dürfen Gemeinden, wie oben ausgeführt, durch Satzung zusätzlich die für die Erhebung des Kurbeitrags erforderlichen Daten auf dem Meldeschein erheben. Der höchstmögliche Kurbeitrag beträgt aber gemäß der dem TLfDI vorgelegten „Satzung über die Erhebung eines Kurbeitrages“ ab einem Alter von 16 Jahren 2,00 Euro/Aufenthaltstag, sodass die Erhebung des Geburtsdatums „Begleitender Ehegatte/Lebenspartner“ für die Erhebung des Kurbeitrages nicht erforderlich war. Der TLfDI bewertete infolgedessen die Erhebung dieses Datums als datenschutzrechtlich unzulässig.
Auch die Erhebung der Geburtsdaten der mitreisenden Kinder auf dem Meldeschein hat der TLfDI für datenschutzrechtlich unzulässig erachtet. Zwar unterscheidet sich der „Kurbeitrag für Kinder unter 7 Jahren“ gemäß Satzung von dem „Kurbeitrag für Kinder von 7 bis 16 Jahren“. Der TLfDI empfahl deshalb, statt der Geburtsdaten der Kinder die „Anzahl der Kinder unter 7 Jahre“ und „Anzahl der Kinder im Alter von 7–16 Jahre“ zu erheben.
Der TLfDI teilte der Stadt weiter mit, dass mittels Meldeschein in keinem Fall die Personalausweisnummer erhoben werden dürfe. Lediglich bei ausländischen Personen muss auf den Meldescheinen gemäß § 30 Abs. 2 Nr. 8 BMG die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapieres verlangt werden.
Abschließend hat der TLfDI darauf hingewiesen, dass es bei einer Verarbeitung und Nutzung der nach § 30 Abs. 2 BMG erhobenen Daten für eine Beherbergungs- oder Fremdenverkehrsstatistik gemäß § 31 BMG auch bei freiwilligen Auskünften - nach dem Thüringer Statistikgesetz (ThürStatG) der Einrichtung einer Statistikstelle (§ 20 ThürStatG) bedürfe.
Die Stadtverwaltung informierte den TLfDI im Anschluss, dass sie die Beherbergungsbetriebe über die ab 1. November 2015 geltende Rechtslage informiert habe und mittlerweile ein – entsprechend den Hinweisen des TLfDI – datenschutzkonformes Layout der Meldescheinvordrucke erstellt worden sei.

Mittels der besonderen Meldescheine für Beherbergungsstätten dürfen grundsätzlich lediglich die in § 30 Abs. 2 BMG aufgeführten Daten von den Beherbergungsstätten erhoben werden. Landesrecht

kann bestimmen, dass für die Erhebung von Fremdenverkehrs- und Kurbeiträgen weitere Daten auf den Meldescheinen erhoben werden dürfen. Diese zusätzlich erhobenen Daten müssen aber für die Erhebung der genannten Beiträge erforderlich sein.

5.14 Nachbarstreitigkeiten und kein Ende in Sicht? – Einhalt durch Datenschutz! – Zum melderechtlichen Auskunftsanspruch

Eine Verwaltungsgemeinschaft (VG) wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat ihn um Rat in folgender Angelegenheit:
Im Bereich Meldewesen der VG war der Hinweis eines Anzeigenden eingegangen, dass ein Bürger sich in einer Wohnung aufhalte, in der er laut Melderegister nicht gemeldet sei. Der zuständige VG-Mitarbeiter habe mit dem Anzeigenden vereinbart, dass bei einer evtl. erforderlichen Anhörung des Betroffenen keine namentliche Benennung des Anzeigenden vorgenommen werde. Nun fordere der Rechtsanwalt des betroffenen Bürgers Akteneinsicht, und es stelle sich die Frage, ob der Bereich Meldewesen auch den Namen des Anzeigenden an den Anwalt übermitteln dürfe. Dies sei in vorliegender Angelegenheit besonders heikel, da hier eine Nachbarschaftsstreitigkeit, eine „Schraube ohne Ende“, vorliege.
Der TLfDI teilte der VG nach Prüfung des Sachverhalts mit, dass er im vorliegenden Fall nicht von einer Übermittlung von Daten, sondern von einem Auskunftsanspruch ausgehe. Auskunft an den Betroffenen (auch an den mandatierten Rechtsanwalt des Bürgers) hat die Meldebehörde auf Antrag nach § 9 Abs. 1 ThürMeldeG zu erteilen. Diese Auskunft erstreckt sich dabei gemäß § 9 Abs. 1 Nr. 1 ThürMeldeG auf alle personenbezogenen Daten und Hinweise des Betroffenen (auch soweit sie sich auf deren Herkunft beziehen), die über ihn im Melderegister, in Akten, Aktensammlungen oder sonstigen Unterlagen der Meldebehörde gespeichert sind. Die Auskunftserteilung unterbleibt, soweit gemäß § 9 Abs. 3 Nr. 3 ThürMeldeG die Daten ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

Der TLfDI informierte die VG ferner über seine Rechtsauffassung, dass die Ablehnung des Auskunftsersuchens des Rechtsanwalts im vorliegenden Fall zulässig sei. Denn hier müsse das Interesse des durch den Rechtsanwalt vertretenen Bürgers hinter das schützenswerte Interesse des Hinweisgebers zurücktreten.
Ergänzend wies der TLfDI die VG darauf hin, dass die Meldebehörde gemäß § 10 Abs. 2 ThürMeldeG verpflichtet sei, bei konkreten Anhaltspunkten für die Unrichtigkeit oder Unvollständigkeit des Melderegisters bezüglich namentlich bekannter Einwohner den Sachverhalt von Amts wegen zu ermitteln. Ob Meldedaten unrichtig sind, bestimmt sich dabei aber ausschließlich nach objektiven Kriterien. Nach der einschlägigen Kommentarliteratur (Medert/Süßmuth/Dette-Koch, Kommentar zum Melderecht des Bundes und der Länder, Erl. zu § 4a MRRG, Rn. 15 bis 19) reichen jedenfalls Vermutungen oder bloße Hinweise, dass Daten unrichtig sein könnten, als „konkrete Anhaltspunkte“ für die Unrichtigkeit des Melderegisters nicht aus.

Zum 1. November 2015 ist das Bundesmeldegesetz (BMG) in Kraft getreten. Das Meldewesen liegt nunmehr in der ausschließlichen Gesetzgebungskompetenz des Bundes. Es ist aber beim gleichlautenden Auskunftsanspruch an die betroffene Person (§ 10 BMG) geblieben.

Bei den Auskunftsansprüchen nach dem Bundesmeldegesetz, wie z. B. gemäß § 10 BMG, kann der Schutz personenbezogener Daten Dritter im Einzelfall dazu führen, dass die melderechtliche Auskunft unterbleibt. Diese Auskunftsbeschränkungen sind in § 11 BMG geregelt. Diese hat die Meldebehörde im Rahmen ihrer Prüfung zu berücksichtigen.

5.15 Unterschriftensammlung – auch hier gilt der Datenschutz

Eine Bürgerinitiative wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und informierte darüber, dass sie Unterschriften für ein Bürgerbegehren gegen ein geplantes Bauprojekt gesammelt hätte. Sofern dabei die Initiative die notwendige (gültige) Zahl an Unterschriften gesammelt und bei der Gemeindeverwaltung eingereicht hat, ist nach § 17 Abs. 5 und 6 Thüringer Kommunalordnung

(ThürKO) ein Bürgerentscheid durchzuführen. Die Bürgerinitiative teilte mit, dass das Landratsamt Schmalkalden-Meiningen auf einer Besprechung die Vorgehensweise der Listenübergabe und Stimmenauszählung bekannt gegeben habe. Dabei erfuhr die Bürgerinitiative insbesondere von einer beabsichtigten Vervielfältigung und Digitalisierung der Eintragungslisten durch das Landratsamt. Dies hielt die Bürgerinitiative für bedenklich.
Aufgrund der Kurzfristigkeit der Angelegenheit wandte sich der TLfDI umgehend an das Landratsamt Schmalkalden-Meiningen und bat um eine Stellungnahme.
Das Landratsamt teilte daraufhin dem TLfDI mit, dass es die Vervielfältigung und Digitalisierung der Eintragungslisten ausschließlich zum Zweck der Prüfung der Wahlberechtigungen der Unterzeichner durchgeführt habe, um diese dann an das jeweils zuständige Einwohnermeldeamt weiterzuleiten. Mit der Feststellung der Zulässigkeit des Bürgerbegehrens seien sämtliche gespeicherte Daten dort unwiederbringlich gelöscht worden.
Es stellte sich dabei die Frage, was mit den ursprünglichen Eintragungslisten passieren sollte. Nach der Aussage des Landratsamtes sollten die Eintragungslisten entsprechend der gesetzlichen Vorgaben der § 17a Abs. 2 Satz 3 ThürKO, § 49 Kommunalwahlordnung (ThürKWO) aufbewahrt werden. Nur der Leiter des Büros Landratsamt könne auf diese Daten zugreifen.
Der § 49 ThürKWO regelt u. a. die Vernichtung von Wahlunterlagen nach Abschluss eines etwaigen Verfahrens zur Wahlprüfung bzw. zur Anfechtung der Feststellung des Wahlergebnisses, nicht aber die Vernichtung von Unterlagen zu Bürgerbegehren im Sinne von § 17 ThürKO. Nachdem jedoch das Bürgerbegehren das erforderliche Unterstützungsquorum erreicht hatte, beschloss der Kreistag, den Bürgerentscheid durchzuführen. Im Ergebnis war damit der erste Verfahrensschritt des Bürgerbegehrens abgeschlossen, sodass eine weitere Aufbewahrung der Daten zu dem abgeschlossenen Verfahren des Bürgerbegehrens nach Ansicht des TLfDI nicht mehr erforderlich war. Aus diesem Grund fragte der TLfDI erneut beim Landratsamt nach, auf welcher Rechtsgrundlage die fortgesetzte Aufbewahrung der Daten des Bürgerbegehrens beruhe und weshalb dies erforderlich sei. Das Landratsamt war der Auffassung, dass die Eintragungslisten zum Bürgerbegehren einer zweijährigen Bindungsfrist nach § 17 Abs. 8 Satz 3 ThürKO unterlägen. Diese Rechtsauffassung teilte der TLfDI nicht. § 17 Abs. 8 Satz 3 ThürKO bezieht sich ledig-

lich auf Bürgerentscheide und regelt, dass ein Bürgerentscheid unter den dort genannten Voraussetzungen innerhalb von zwei Jahren nur durch einen neuen Bürgerentscheid abgeändert werden kann. Dass ein Bürgerbegehren und ein Bürgerentscheid in datenschutzrechtlicher Hinsicht eigenständig zu betrachten sind, ergibt sich unter anderem mittels Vergleichs mit der Datenschutznorm in § 5 des Thüringer Gesetzes über Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG). Danach dürfen personenbezogene Daten, die auf der Grundlage dieses Gesetzes erhoben werden, nur für die Durchführung des jeweiligen Antrags auf Zulassung eines Volksbegehrens oder Volksentscheids verarbeitet oder genutzt werden. Werden sie für das Verfahren nicht mehr benötigt, sind sie unverzüglich zu vernichten.
Der TLfDI vertrat deshalb im Ergebnis die Rechtsauffassung, dass die Eintragungslisten zum Bürgerbegehren mit den darin enthaltenen personenbezogenen Daten nach dem erfolgten Kreistagsbeschluss zur Durchführung des Bürgerentscheides entsprechend § 16 Thüringer Datenschutzgesetz (ThürDSG) zu löschen waren und forderte das Landratsamt Schmalkalden-Meiningen auf, entsprechend zu handeln. Unter Berücksichtigung von § 4 Abs. 1 Satz 2 Thüringer Archivgesetz, der die Archivierung kommunalen Archivguts durch Gemeinden, Landkreise und kommunale Verbände in eigener Verantwortung und Zuständigkeit regelt, ist vom Gesetzgeber hier eine Klarstellung in der ThürKO zu verlangen, dass personenbezogene Daten aus Eintragungslisten von Bürgerbegehren unverzüglich zu löschen sind, sobald sie für das Verfahren zum konkreten Bürgerbegehren nicht mehr benötigt werden.
Daraufhin teilte das Landratsamt dem TLfDI mit, dass sämtliche Unterschriftslisten zum Bürgerbegehren vernichtet wurden. Der TLfDI sah infolgedessen die Angelegenheit als erledigt an.

Nach § 17 ThürKO können Bürger über wichtige Angelegenheiten des eigenen Wirkungskreises der Gemeinde die Durchführung eines Bürgerentscheids beantragen (Bürgerbegehren). Für ein erfolgreich zu Stande gekommenes Bürgerbegehren wird jedoch eine gewisse Anzahl an Unterschriften benötigt. Auch eine Unterschrift ist ein personenbezogenes Datum im Sinne vom § 3 Abs. 1 ThürDSG, da es eine Einzelangabe über das persönliche Verhältnis einer bestimmten natürlichen Person ist. Personenbezogene Daten sind grundsätzlich gemäß § 16 ThürDSG unter anderem dann zu löschen, wenn ihre

Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Das war bei den Eintragungslisten nach Abschluss des Bürgerbegehrens der Fall.

5.16 Thüringer Landeswahlordnung – Klappe, die Vierte (Änderung)

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm Anfang des Jahres 2014 Stellung zu einem Entwurf der vierten Änderung der Thüringer Landeswahlordnung (ThürLWO). Der Verordnungsentwurf sollte die notwendigen Folgeänderungen, die sich aus dem Fünften Gesetz zur Änderung des Landeswahlgesetzes vom 22. März 2012 ergeben hatten, vornehmen. Darüber hinaus sollte die Verordnung die zwischenzeitlich erfolgten Änderungen der Bundeswahlordnung aufgreifen, sodass die Landeswahlordnung nach dem Grundsatz der Harmonisierung des Wahlrechts des Bundes und der Länder an die Bundeswahlordnung anzupassen war. Die Änderungen betrafen im Wesentlichen die Abschaffung von Antragsgründen für die Beantragung der Briefwahl, die Anpassung von Begrifflichkeiten sowie die Harmonisierung des Wahlrechts des Bundes und der Länder.
Der TLfDI begrüßte aus datenschutzrechtlicher Sicht, dass nunmehr die Wahlscheine unmittelbar an den Wahlberechtigten übersandt werden sollten. Die Zustimmung des TLfDI fand auch, dass im Wählerverzeichnis gemäß § 19 Abs. 2 des Entwurfes der Vierten Verordnung zur Änderung der Thüringer Landeswahlordnung (ThürLWO-E) während der Auslegungsfrist die Wohnung (Anschrift) für Wahlberechtigte, für die im Wählerverzeichnis eine Auskunftssperre gemäß § 31 Abs. 7 Thüringer Meldegesetz (nunmehr § 51 Bundesmeldegesetz [BMG]) eingetragen ist, von Amts wegen unkenntlich zu machen war. Der TLfDI gab hierzu aber den Hinweis zu prüfen, ob in § 19 ThürLWO-E die Unkenntlichmachung lediglich der Wohnung und nicht zum Beispiel auch des Geburtsdatums von Amts wegen aufgrund des Zweckes des damals geltenden § 31 Abs. 7 Thüringer Meldegesetz (Auskunftssperre bei der Möglichkeit der Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen des Betroffenen oder einer anderen Person) zum Schutz des Betroffenen dienlich wäre. Es blieb jedoch dabei, dass im Wählerverzeichnis während der Auslegungsfrist von Amts wegen zunächst nur die Wohnung (Anschrift) von Wahlberechtigten,

für die im Melderegister eine Auskunftssperre nach § 51 Abs. 1 Bundesmeldegesetz (BMG) eingetragen ist, unkenntlich zu machen ist.

In § 19 Abs. 2 Thüringer Landeswahlordnung (ThürLWO) heißt es nunmehr:
„Im Wählerverzeichnis ist während der Auslegungsfrist die Wohnung von Wahlberechtigten, für die im Melderegister eine Auskunftssperre nach § 51 Abs. 1 BMG eingetragen ist, von Amts wegen unkenntlich zu machen. Auf Verlangen des Wahlberechtigten ist in dem Wählerverzeichnis während der Auslegungsfrist das Geburtsdatum unkenntlich zu machen."

5.17 Leck im Rathaus Nordhausen? – personenbezogene Daten im Netz

Wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) der Presse entnehmen konnte, war eine Liste der Stadtverwaltung Nordhausen zu Geschwindigkeitsmessungen mit personenbezogenen Daten der daran beteiligten Mitarbeiter von privater Seite in das soziale Netzwerk Facebook gestellt worden. Bei einer solchen Veröffentlichung handelt es sich um eine unbefugte Übermittlung personenbezogener Daten.
Daraufhin bat der TLfDI die Stadtverwaltung Nordhausen mitzuteilen, wie es zu diesem Vorfall kommen konnte und welche technisch-organisatorischen Maßnahmen eingeleitet wurden, um künftig ähnliche Vorkommnisse auszuschließen.
Die Stadtverwaltung Nordhausen teilte mit, dass die veröffentlichten Daten aus den bei der Verfolgung von Verkehrsordnungswidrigkeiten an die betreffenden Fahrzeughalter übersandten Fragebögen stammten, da hierin die als Zeuge der Feststellung von Verkehrsordnungswidrigkeiten beteiligten Mitarbeiter der Stadtverwaltung mit Anrede und Nachnamen genannt würden.
Nach Auffassung der Stadtverwaltung Nordhausen gehörte der Versand von Fragebögen an die Fahrzeughalter zum nichtförmlichen Verwarngeld-Vorverfahren. Im Unterschied zum förmlichen Bußgeldverfahren sei hierbei die Übermittlung von personenbezogenen Daten der beteiligten Mitarbeiter nicht erforderlich. Daher beabsichtigte die Stadtverwaltung, in den o. g. Fragebögen künftig anstelle von Anrede und Nachname lediglich Pseudonyme ihrer Mitarbeiter

anzugeben. Das Pseudonymisieren ist gemäß § 3 Abs. 10 ThürDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch Kenzeichen zu dem Zweck, die Bestimmung des Betroffenen ohne Nutzung der Zuordnungsfunktion auszuschließen oder wesentlich zu erschweren.
Diese Vorgehensweise stellt aus Sicht des TLfDI eine geeignete organisatorische Maßnahme dar, um zur Erhöhung des Datenschutzniveaus im öffentlichen Bereich zu gelangen.

Damit öffentliche Stellen im Zeitalter von Facebook und Co. die personenbezogenen Daten ihrer Mitarbeiter im erforderlichen Umfang schützen können, bietet sich das Pseudonymisieren von Namen oder anderen Identifikationsmerkmalen gemäß § 3 Abs. 10 ThürDSG an. Auf diese Weise können die öffentlichen Stellen Gewähr dafür bieten, dass eine unzulässige Datenübermittlung personenbezogener Daten von vornherein unmöglich wird.

5.18 Mit Speck fängt man Mäuse – Stadtwerke bieten Anreize für werbliche Nutzung von Kundendaten

Die Stadtwerke Erfurt Gruppe (SWE Gruppe) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum um datenschutzrechtliche Beratung zu ihrem Vorhaben, für Neubürger der Stadt Erfurt ein Willkommenspaket in Form eines Bonusheftes mit unentgeltlichen Leistungen auszugeben. Um das Bonusheft zu erhalten, sollte der Neukunde einen Strom- oder Gaslieferungsvertrag mit der SWE Energie GmbH für mindestens ein Jahr abschließen und in eine konzernweite Nutzung seiner Namens- und Adressdaten zur werblichen Ansprache per Post durch die Konzernunternehmen der SWE Gruppe einwilligen.

Zu dem Vorhaben vertrat der TLfDI folgende Auffassung:
Das Kopplungsverbot nach § 28 Abs. 3b Bundesdatenschutzgesetz (BDSG) verbietet es der verantwortlichen Stelle, den Abschluss eines Vertrags von einer Einwilligung des Betroffenen zur werblichen Datennutzung abhängig zu machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.
Hier wird der Erhalt der Boni unter die Voraussetzung der Einwilligung in die werbliche Nutzung von Kundendaten gestellt, wobei

jedoch die angebotenen Leistungen auch ohne Einwilligung in die Preisgabe von Kundendaten zu Werbezwecken erlangt werden können. Nach Ansicht der Kommentarliteratur ist es zulässig, den Betroffenen durch einen positiven Anreiz in Form einer Zusatzleistung zur Abgabe einer Einwilligung bewegen zu wollen. Das Paradebeispiel für diese Praxis sind Bonus- oder Treuepunktsysteme. In der Tat ist hierbei die Abgabe der Einwilligung nicht mit der Abwendung eines Nachteils, sondern mit der Gewährung eines Vorteils verbunden. Der Betroffene wird nicht in seiner Willensfreiheit beeinträchtigt. Er entscheidet sich vielmehr bewusst für die Verwendung seiner Daten zu Werbezwecken, um in den Genuss der versprochenen Leistung zu kommen (vgl. Kai-Uwe Plath, Kommentar zum BDSG sowie den Datenschutzbestimmungen des TMG und TKG, Anmerkung 174 zu § 28 Abs. 3b BDSG, Seite 623).
Insoweit unterliegt die vorgesehene Gewährung von Bonusleistungen in Abhängigkeit von einer Einwilligung in die konzernweite Nutzung der Namens- und Adressdaten zur werblichen Ansprache durch die Konzernunternehmen der SWE Gruppe nicht dem Kopplungsverbot im Sinne von § 28 Abs. 3b BDSG. Die vorgelegte schriftliche Einwilligungserklärung entsprach den datenschutzrechtlichen Anforderungen.

Stadtwerke haben bei ihrem Marketing die rechtlichen Voraussetzungen des Bundesdatenschutzgesetzes zu beachten. Die vorgesehene Bonusgewährung mittels des Willkommenspakets der Stadtwerke Erfurt unterlag nicht dem gesetzlichen Kopplungsverbot und war daher zulässig.

5.19 Video(attrappen)gaga 1

Die Stadt Erfurt teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum mit, dass zum Schutz öffentlichen Eigentums vor Diebstahl auf ihrem Betriebsgelände zunächst eine Kameraattrappe und später eine „echte“ Kamera außerhalb der Dienstzeiten eingesetzt werden solle. Für den späteren „Echtzeitbetrieb“ der Kamera sei ausgeschlossen, dass sich in dieser Zeit auf dem Gelände Bedienstete aufhalten dürfen.

Da der Stadt Erfurt die Rechtslage bei Videoüberwachungen bekannt war, beschränkte sich der TLfDI auf die folgenden Hinweise zum Einsatz von Kameraattrappen:
Kameraattrappen sind so zu beurteilen, als ob unter den gegebenen Umständen eine echte Videoüberwachung durchgeführt würde. Da diese Maßnahme im konkret zu beurteilenden Fall auf einen nicht öffentlich zugänglichen Bereich und auf die Zeiten außerhalb der Arbeitszeit beschränkt war, waren schutzwürdige Interessen der Beschäftigten nicht tangiert. Daher sah der TLfDI den Einsatz einer Kameraattrappe unter den o. g. Voraussetzungen als zulässig an.
Die Maßnahme der Videoüberwachung – so die Aufforderung des TLfDI – sollte aber mittels eines Piktogramms und der Angabe der verantwortlichen Stelle erkennbar gemacht werden. Einen zeitlichen Hinweis über den Einsatz der Videoüberwachung hielt der TLfDI nicht für erforderlich.
Bei der Beteiligung des Personalrates nach § 74 Abs. 2 Nr. 11 Thüringer Personalvertretungsgesetz handelte es sich um eine Frage des Personalvertretungsrechts, nicht des Datenschutzrechts. Aus datenschutzrechtlicher Sicht war der Personalrat aber zumindest darüber in Kenntnis zu setzen, dass keine Videoüberwachung innerhalb der Arbeitszeit stattfinde.
Eine Dokumentation gemäß § 10 Thüringer Datenschutzgesetz (ThürDSG) war nach Auffassung des TLfDI nicht erforderlich. Jedoch sollten beim Verfahrensverzeichnis die erforderlichen Angaben bezüglich der Kameraattrappe dokumentiert werden, um der Auskunftspflicht im Sinne vom § 10 Abs. 3 ThürDSG nachkommen zu können.
Der behördliche Datenschutzbeauftragte war schließlich auch in Fällen des Einsatzes von Kameraattrappen zu beteiligen.

Auch Kameraattrappen stellen einen Eingriff in die Privatsphäre und in das Recht auf informationelle Selbstbestimmung dar. Denn eine Person, die nicht weiß, dass die Kameraattrappe gar keine Videobeobachtung oder -aufzeichnung ermöglichen kann, wird sich daher möglicherweise anders verhalten, als wenn sie sich völlig unbeobachtet fühlt. Daher sind Kameraattrappen in datenschutzrechtlicher Hinsicht wie echte Videoüberwachungsmaßnahmen zu beurteilen.

5.20 Die Nadel im Heuhaufen – wie findet man einen datenschutzkonformen Entsorger?

Eine Stadtverwaltung wollte vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wissen, wie ein datenschutzkonform handelndes Unternehmen für die Entsorgung dienstlichen Schriftgutes ausgewählt werden kann.

Nach § 3 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) umfasst die Verarbeitung personenbezogener Daten auch deren Löschung, die naturgemäß mit der Entsorgung bzw. Vernichtung von Schriftgut verbunden ist. Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt gemäß § 8 ThürDSG der Auftraggeber für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung für die jeweils zum Einsatz kommenden technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und erforderlichenfalls alle Unterauftragsverhältnisse schriftlich festzulegen sind. Entsprechendes gilt auch für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen, soweit ein Zugriff auf personenbezogene Daten dabei nicht ausgeschlossen werden kann. In diesem Zusammenhang weist der TLfDI auf den in der Anlage 23 seines 5. Tätigkeitsberichts veröffentlichten Mustervertrag zur Auftragsdatenverarbeitung hin.
Jedoch gibt es keine datenschutzrechtlichen Vorgaben, wonach unternehmensbezogene Zertifikate als Entscheidungskriterium im Sinne eine „K.o.-Kriteriums“ zur Auftragsvergabe heranzuziehen sind, zumal durch ein solches Vorgehen Unternehmen, die nicht zertifiziert wurden, jedoch die geforderte Eignung besitzen, vom Vergabeverfahren ausgeschlossen wären. Ggf. sollten Nachweise zu einem Datenschutzaudit nach § 9a Bundesdatenschutzgesetz (BDSG) als ein Orientierungsmerkmal zur fachlichen Beurteilung der Unternehmen herangezogen werden. Der Auftraggeber sollte sich in jedem Fall von den infrage kommenden Unternehmen Nachweise zur Umsetzung der §§ 4 ff. BDSG vorlegen lassen und sich darüber informieren, ob die potentiellen Auftragnehmer datenschutzrelevante

technische Richtlinien erfüllen. So beschreibt die DIN 66399-1 die Anforderungen an Maschinen und Einrichtungen zur Vernichtung von Informationsträgern (Papier und Mikrofilm). Obwohl sie keine Rechtsnorm ist, liefert sie Anhaltspunkte für das im Einzelfall erforderliche Sicherheitsmaß bei der Vernichtung. Je nach dem Grad der Schutzbedürftigkeit der auf dem Datenträger gespeicherten Informationen werden fünf Sicherheitsstufen definiert. Die Sicherheitsstufe drei (z. B. Streifenbreite max. 2 mm bei beliebiger Länge des vernichteten Papiers) sollte eine Mindestanforderung für eine datenschutzgerechte Vernichtung sein. Für sensible personenbezogene Daten, wie Pass- und Meldedaten sowie Personaldaten, ist nach DIN 66399-1 eine Sicherheitsstufe größer vier erforderlich.

Abgesehen von den Regelungen zur Auftragsdatenverarbeitung gibt es keine speziellen gesetzlichen Normen zur Auswahl von Entsorgungsunternehmen. Jedoch bieten Nachweise über die Einhaltung von Vorgaben des Bundesdatenschutzgesetzes und zu entsorgungstechnischen Normen sowie Datenschutzaudits und Zertifikate praktikable Selektionskriterien.

5.21 Dürfen personenbezogene Daten von Wahl-Kandidaten ins Internet?

Ein behördlicher Datenschutzbeauftragter beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum über die Veröffentlichung von Geburtsdaten der Kandidaten zur Kommunalwahl im Jahr 2009 auf der Internetseite des Thüringer Landesamts für Statistik (TLS).
Der TLfDI vertrat hierzu die Auffassung, dass eine Veröffentlichung personenbezogener Daten von Kandidaten zur Kommunalwahl im Internet mangels einer geeigneten Rechtsgrundlage nicht zulässig sei. Zu dieser Frage vom TLfDI zur Stellungnahme aufgefordert, teilte das TLS mit, dass es die Geburtsdaten der Kandidaten für die Kommunalwahlen 2014 nicht ins Internet einstellen werde. Diese Zusage wurde eingehalten.
Jedoch stellte der TLfDI im Falle der Landtagswahl 2014 fest, dass das TLS und die Stadt Erfurt die personenbezogenen Daten (Name, Vorname, Geburtsjahr, Wohnanschrift, Beruf) der Bewerber der zugelassenen Landeslisten bzw. Wahlkreisvorschläge auf ihren Internetseiten veröffentlicht hatten. Da auch in diesen Fällen eine ge-

eignete Rechtsgrundlage für derartige Internetveröffentlichungen nicht ersichtlich war, erfolgte die Veröffentlichung o. g. Daten in unzulässiger Weise. Konkret handelte es sich bei dieser Veröffentlichung um einen Verstoß gegen § 23 Thüringer Datenschutzgesetz (Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes). Der TLfDI forderte die betroffenen Stellen auf, zu der Angelegenheit Stellung zu nehmen und die Veröffentlichungen personenbezogener Daten aus dem Netz zu nehmen.

Das TLS führte in seiner Stellungnahme u. a. aus, dass § 67 Abs. 3 Thüringer Landeswahlgesetz (ThürLWG), wonach der Landeswahlleiter die Öffentlichkeit unter der angegebenen Internetadresse über die Landtagswahl informiert – eine geeignete Rechtgrundlage auch für die Veröffentlichung personenbezogener Daten der Kandidaten der Landtagswahl im Internet darstelle. Die Stadt Erfurt teilte dem TLfDI mit, dass der Kreiswahlleiter der Wahlkreise 24 bis 27, Erfurt I bis IV, entgegen der Beurteilung des TLfDI weiterhin von einer Zulässigkeit der o. g. Internetveröffentlichung ausgehe.

Der TLfDI entgegnete, dass die Regelung des § 67 Abs. 3 ThürLWG aufgrund ihrer systematischen Einordnung im zehnten Abschnitt des ThürLWG (Wahlkosten und Wahlstatistik) keine hinreichend bestimmte Rechtgrundlage für eine Veröffentlichung personenbezogener Daten der Kandidaten der Landtagswahl im Internet darstelle. Vielmehr sei anzunehmen, dass die Rechtsnorm lediglich statistischen Veröffentlichungen im Zusammenhang mit Wahlen dienen soll. Dies ergebe sich insbesondere daraus, dass die genannte Regelung im vierten Abschnitt des Gesetzes (Vorbereitung der Wahl) des ThürLWG gerade nicht enthalten sei. An dieser rechtlichen Bewertung ändere auch die Möglichkeit nichts, dass die nach dem ThürLWG und der Thüringer Landeswahlordnung (ThürLWO) vorgesehenen Daten der Kandidaten der Landtagswahl nach § 81 Nr. 1 und 2 ThürLWO im Thüringer Staatsanzeiger zu veröffentlichen sind und der Thüringer Staatsanzeiger im Internet abgerufen werden kann.

Nachfolgend regte der TLfDI gegenüber dem damaligen Thüringer Justizministerium (TJM) an, für den o. g. Sachverhalt eine präzisere Rechtgrundlage, etwa im vierten Abschnitt des ThürLWG, zu implementieren.

Hierzu teilte das TJM dem TLfDI u. a. mit, dass eine solche Veröffentlichung im Internet nicht von den Regelungen des

§ 81 ThürLWO zur öffentlichen Bekanntmachung gedeckt sei. Ob § 67 Abs. 3 ThürLWG für Namen und für weitere personenbezogene Daten eine taugliche Grundlage biete, sei nicht abschließend zu beantworten. Die Norm spreche weder eindeutig dafür noch eindeutig dagegen. Eine Veröffentlichung wäre allerdings nicht zu kritisieren, wenn die Bewerber einer Veröffentlichung weiterer personenbezogener Daten zugestimmt hätten. Es sollte jedoch insgesamt Beachtung finden, für welchen Adressatenkreis solche Daten tatsächlich zur Verfügung zu stellen sind. Es sei dabei die Frage zu beantworten, ob es sich um einen eingeschränkten Adressatenkreis handele, wie etwa den Landeswahlleiter bzw. das TLS, oder ob (über das Internet) ein völlig unbeschränkter Adressatenkreis zu berücksichtigen sei. lm Zweifel sollte eher eine restriktive Handhabung erfolgen. Dem zuständigen Thüringer Ministerium für Inneres und Kommunales (TMIK) obliegt es nunmehr, eine klarstellende gesetzgeberische Entscheidung herbeizuführen.

Da nach derzeitiger Rechtslage eine Veröffentlichung personenbezogener Daten von Wahlkandidaten im Internet unzulässig ist, sollte das TMIK das „Heft des Handelns“ in die Hand nehmen und dafür sorgen, dass sowohl das Thüringer Kommunalwahlgesetz als auch das Thüringer Landeswahlgesetz um jeweils eine eindeutige Rechtsgrundlage ergänzt werden, die eine solche Veröffentlichung zulässt.

5.22 Eine amtliche E-Mail als lehrreiches Eigentor

Das Ordnungsamt einer Stadtverwaltung hatte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum eine Ordnungswidrigkeiten-Anzeige nebst Anlagen mit den darin enthaltenen personenbezogenen Daten per E-Mail in unverschlüsselter Form übersandt.
Aus diesem Anlass wies der TLfDI die verantwortliche Stadtverwaltung darauf hin, dass für die Zulässigkeit einer Datenübermittlung personenbezogener Daten an eine andere öffentliche Stelle die übermittelnde Stelle verantwortlich ist (§ 21 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG)). Nach § 9 i. V. m. § 3 Abs. 3 ThürDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, auf der Grundlage eines Sicherheitskonzeptes die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses

Gesetzes zu gewährleisten. Hierzu zählen gemäß § 9 Abs. 2 Nr. 1 bis 6 ThürDSG die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und die Transparenz. Um diese Ziele auch bei der Datenübermittlung von personenbezogenen Daten über den unsicheren Übertragungsweg per E-Mail zu gewährleisten, ist sicherzustellen, dass Unbefugte durch geeignete Verschlüsselungsverfahren die Daten nicht zur Kenntnis nehmen können. Kann die öffentliche Stelle dies nicht gewährleisten, so hat sie den (sicheren) Postweg zu nutzen.
Im Ergebnis stellte der TLfDI fest, dass eine unverschlüsselte Übermittlung personenbezogener Daten mittels des unsicheren Übertragungsweges per E-Mail gegen datenschutzrechtliche Bestimmungen verstößt und bat, dafür Sorge zu tragen, dass die o. g. Hinweise künftig in der verantwortlichen Stadtverwaltung beachtet werden. Zugleich bat der TLfDI, ihm die Regelungen der Stadtverwaltung zum Umgang mit elektronischer Kommunikation (E-Mail) zu übersenden. Daraufhin teilte die Stadtverwaltung dem TLfDI mit, dass die unverschlüsselte E-Mail aus Versehen übersandt worden sei und sie zukünftig die datenschutzrechtlichen Vorgaben beachte. Der TLfDI stellte fest, dass vorgelegte Regelung der Stadtverwaltung zum Umgang mit elektronischer Kommunikation (E-Mail) den datenschutzrechtlichen Vorgaben entsprach.

Alle öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben gemäß § 9 Abs. 1 Satz 1 ThürDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen des Thüringer Datenschutzgesetzes zu gewährleisten. Danach hat z. B. eine Kommune ihren alltäglichen Umgang mit Kommunikationsmitteln regelmäßig kritisch zu prüfen und sich daran zu erinnern, dass das Senden unverschlüsselter E-Mails, die personenbezogene Daten enthalten, gegen den Grundsatz der Vertraulichkeit gemäß § 9 Abs. 2 Satz 1 Nr. 2 ThürDSG verstößt. Daher sollte der Postweg als sicherere Übermittlungsform gewählt werden.

5.23 Hunger des Landratsamtes Saale-Orla-Kreis auf Grundsteuerdaten

Wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum erfuhr, begehrte

das Landratsamt des Saale-Orla-Kreises zur Mietwerterhebung zum Zwecke der Feststellung der Angemessenheitsgrenzen der Kosten der Unterkunft für Leistungsempfänger nach dem SGB II und SGB XII von der Stadtverwaltung Bad Lobenstein die Anzahl der Grundeigentümer, die Adressdaten kleiner Vermieter, bei denen vermutet wurde, dass diese Wohnraum vermieten, sowie die Adressen etwaiger Mietobjekte.
Nach datenschutzrechtlicher Prüfung vertrat der TLfDI im konkreten Fall die Auffassung, dass eine Übermittlung der Anzahl der potentiellen Vermieter keinen datenschutzrechtlichen Bedenken begegnet.
Nach § 31 Abs. 3 Abgabenordnung (AO) dürfen Gemeinden Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekannt geworden sind, zur Verwaltung anderer Aufgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben verwenden. Sofern nicht schutzwürdige Verhältnisse des Betroffenen überwiegen, dürfen diese Verhältnisse auch den zuständigen Gerichten, Behörden und anderen juristischen Personen des öffentlichen Rechts offenbart werden. Da ein Überwiegen schutzwürdiger Interessen der betroffenen Grundstückseigentümer gegenüber der Aufgabe des Landratsamtes zur Mietwerterhebung zum Zwecke der Feststellung der Angemessenheitsgrenzen der Kosten der Unterkunft für Leistungsempfänger nach dem SGB II und SGB XII nicht ersichtlich war, war eine Übermittlung der Namen und Anschriften von Grundstückeigentümer zu dem o. g. Zweck zulässig.
Anders stellte sich die Rechtslage nach Auffassung des TLfDI für die Übermittlung von Adressen etwaiger Mietobjekte dar:
Mangels einer geeigneten Rechtgrundlage war eine Übermittlung der Adressen etwaiger Mietobjekte nicht zulässig. § 31 Abs. 3 AO war in diesem Fall nicht anwendbar, da danach nur Name und Anschrift der Grundstückseigentümer mitgeteilt werden dürfen und somit bei der gebotenen restriktiven Auslegung dieser Norm kein Raum für die Übermittlung weiterer Datenarten bestand.
Zur Frage, ob sich öffentliche Stellen privater Dienstleister zur Verarbeitung von Steuerdaten zur Mietwerterhebung, etwa im Wege der Auftragsdatenverarbeitung, bedienen dürfen, vertrat der TLfDI folgende Auffassung:
Der Anwendungsbereich der AO wird nach § 15 Thüringer Kommunalabgabengesetz (ThürKAG) eröffnet. Hier ist geregelt, dass für Kommunalabgaben die Abgabenordnung anzuwenden ist, soweit gesetzlich nichts anderes bestimmt ist. Insbesondere ist damit

§ 30 AO für das Steuergeheimnis anzuwenden. Eine Regelung, wonach sich Gemeinden oder Gemeindeverbände für die Durchführung o. g. Aufgaben privater Dritter als Verwaltungshelfer bedienen können, enthält das ThürKAG nicht. Daher ist im kommunalen Bereich davon abzusehen, privaten Dienstleistern den Zugang zu Steuerdaten zu ermöglichen. Grundsätzlich ist jedoch die Einbeziehung privater Dritter bei der Mietwerterhebung unter bestimmten Voraussetzungen als zulässig anzusehen. Nähre Ausführungen zu dieser Thematik finden sich unter dem Gliederungspunkt 5.4. des 9. Tätigkeitsberichts des TLfDI.

Bei der zweckändernden Nutzung von Grundsteuerdaten sind die spezialgesetzlichen Regelungen der Abgabenordnung, insbesondere von § 31 Abs. 3 AO hinsichtlich des zulässigen Datenumfangs, restriktiv auszulegen. Die Einbeziehung privater Dienstleister bei der Mietwerterhebung ist nur unter engen Voraussetzungen als zulässig anzusehen.

5.24 Mystery-Check im Thüringer Wald

Bereits im Mai 2013 hatte die Tourismus GmbH Oberhof ein Privatunternehmen vertraglich mit der Erhebung von Daten zur Servicequalität beauftragt. Bei diesen so genannten Mystery-Calls bzw. Mystery-Checks wird den Zimmervermietern per Telefon oder E-Mail vorgegaukelt, dass ein Kunde ein Zimmer mieten will. In Wirklichkeit soll jedoch die Servicequalität seines Unternehmens am Telefon oder per E-Mail beurteilt werden. Im Einzelnen waren monatlich 750 solcher Anrufe und E-Mails bei 250 Zimmervermietern der Region Oberhof vorgesehen. „Gegenstand der Erhebung, Verarbeitung und Nutzung personenbezogener Daten“ sollten laut Vertrag Personenstammdaten und Kommunikationsdaten (z. B. Telefon, E-Mail) sein. Nachfolgend beschloss die Kommunale Arbeitsgemeinschaft Ferienregion Oberhof (KAG) die Erfassung der Servicequalität der Beherbergungsbetriebe in der Ferienregion Oberhof mittels des Verfahrens „Mystery-Check“. Der KAG gehören die Städte Oberhof, Suhl (OT Goldlauter-Heidersbach), Zella-Mehlis und Steinbach-Hallenberg sowie die Gemeinden Frankenhain, Gehlberg, Oberschönau, Unterschönau, Luisenthal und Crawinkel an.
Infolge einer Beschwerde recherchierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI),

dass die betroffenen Mitarbeiter und Inhaber der Beherbergungsbetriebe vorab nicht um ihre Einwilligung zur Erhebung ihrer personenbezogenen Daten gebeten wurden. In einer Pressemitteilung hatte die KAG u. a. lediglich ausgeführt, „… dass selbstverständlich die strengen Auflagen des Datenschutzes beachtet und keine personenbezogenen Details erhoben werden."

Der TLfDI hat den festgestellten Sachverhalt wie folgt bewertet:

Beim Verfahren „Mystery-Check" wurden personenbezogene Daten im Sinne von § 3 Abs. 3 ThürDSG verarbeitet. Bei den erhobenen Daten handelte es sich um personenbezogene bzw. personenbeziehbare Einzelangaben über das Kommunikationsverhalten von Inhabern und Mitarbeitern von Beherbergungsbetrieben im Sinne des § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG).

Im Auftrag der KAG (Auftraggeber) hatte die Tourismus GmbH Oberhof (Auftragnehmer) ein Privatunternehmen (Unterauftragnehmer) mit der Durchführung der Datenerhebung und Datenverarbeitung beauftragt. Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt der Auftraggeber für die Einhaltung der Bestimmungen datenschutzrechtlicher Vorschriften verantwortlich, § 8 Abs. 1 ThürDSG. Daher blieben die zehn in der KAG zusammengeschlossenen Gemeindeverwaltungen verantwortliche Stellen für die von ihnen veranlasste Erhebung und Verarbeitung personenbezogener Daten.

Eine solche Erhebung personenbezogener Daten ist gemäß § 19 Abs. 1 ThürDSG nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Fraglich war im vorliegenden Sachverhalt aber bereits, ob es Aufgabe der Gemeindeverwaltungen als KAG-Mitglieder war, die Service-Qualität privater Beherbergungsbetriebe zu bewerten.

Der Begriff „Erforderlichkeit" ist ein unbestimmter Rechtsbegriff, der im jeweiligen Einzelfall auszufüllen und zu konkretisieren ist. Hierbei ist zu beachten, dass das Datenschutzrecht von dem Grundsatz geprägt ist, dass Datenerhebung, -verarbeitung und -nutzung grundsätzlich verboten sind. Für ihre Zulässigkeit bedarf es einer Erlaubnisnorm oder einer Einwilligung der betroffenen Personen. Daraus folgt ein strenger Maßstab für die Beurteilung der Erforderlichkeit einer Datenerhebung. Dabei ist auch zu berücksichtigen, dass es in Zeiten vielfältig genutzter automatisierter Datenverarbeitung kein „belangloses" Datum mehr gibt, dessen Erhebung quasi

unbedeutend wäre. Die Kenntnis der Daten ist dann erforderlich, wenn die öffentliche Stelle im jeweiligen konkreten Einzelfall ihre Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und außerdem erst aktuell dann und nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person erfordert (Sokol in Simitis, Bundesdatenschutzgesetz, 6. Auflage, § 13, Randnummern 25 und 26).
Letztlich konnte die Frage, ob die Datenerhebung im vorliegenden Sachverhalt erforderlich war, jedoch offen bleiben. Denn im konkreten Fall waren die weiteren Voraussetzungen des § 19 Abs. 2 ThürDSG für eine Datenerhebung durch die KAG, bzw. ihre Mitgliedskommunen nicht gegeben. Nach § 19 Abs. 2 Satz 1 ThürDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Dies setzt voraus, dass der Betroffene an der Erhebung seiner Daten bewusst mitwirkt, d. h., dass ihm die Tatsache einer Datenerhebung und der damit verbundene Eingriff in seine Persönlichkeitsrechte bekannt sein müssen. Dies war hier gerade nicht der Fall. Denn nach Feststellungen des TLfDI hatte das beauftragte Unternehmen zunächst drei verschiedene Gesprächsszenarien mit den Tourismusbetrieben entwickelt. In einem dieser drei Gesprächsszenarien suggerierte ein Mitarbeiter des beauftragten Unternehmens, dass er Zimmer bzw. Zimmerkontingente bei dem angerufenen Tourismusbetrieb buchen bzw. reservieren wolle. Während dieses Gesprächs wurde dann – ohne Wissen des Gesprächspartners des angerufenen Tourismusbetriebes – vom Mitarbeiter des Unternehmens anhand einer Matrix mit vorab definierten Bewertungskriterien das Verhalten des Gesprächspartners des Tourismusbetriebes am Telefon bewertet. Ohne Mitwirkung des Betroffenen dürfen dessen personenbezogene Daten aber nur erhoben werden, wenn 1. dies eine Rechtsvorschrift vorsieht oder zwingend voraussetzt (§ 19 Abs. 2 Satz 1 Nr. 1 ThürDSG), 2. die erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht (§ 19 Abs. 2 Satz 1 Nr. 2 ThürDSG) oder 3. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (§ 19 Abs. 2 Satz 1 Nr. 3 ThürDSG). In den Fällen der genannten Nr. 2 und Nr. 3 ist eine Erhebung bei Dritten nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Im konkreten Fall war hier weder eine Rechtvorschrift im Sinne des § 19 Abs. 2 Nr. 1 ThürDSG ersichtlich, auf die diese Datenerhebung gestützt werden konnte, noch konnte angenommen werden, dass eine Verwaltungsaufgabe einen derartigen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Inhaber und Mitarbeiter der befragten Unternehmen zwingend voraussetzte bzw. erforderlich machte. Da im Ergebnis nicht erkennbar war, dass die Zulässigkeitsvoraussetzungen des § 19 Abs. 2 ThürDSG vorlagen, stellte die Erhebung und Verarbeitung von personenbezogenen Daten mittels des Verfahrens „Mystery-Check“ einen Verstoß gegen datenschutzrechtliche Vorschriften dar.
Aufgrund dieser Bewertung beanstandete der TLfDI die rechtswidrige Erhebung und Verarbeitung personenbezogener Daten von Beherbergungsunternehmen schließlich gegenüber den für die unzulässige Datenerhebung verantwortlichen Mitgliedsgemeinden des KAG gemäß § 39 Abs. 1 Satz 1 ThürDSG. Der TLfDI unterrichtete ferner die für die betroffenen Gemeindeverwaltungen zuständigen Kommunalaufsichten des Ilm-Kreises, der Landkreise Gotha und Schmalkalden-Meiningen sowie der Stadt Suhl von der o. g. Beanstandung. Abschließend wurden dem TLfDI die Protokolle zum Nachweis der erfolgten Löschung der unrechtmäßig erhobenen Daten vorgelegt.

Der Fall Mystery-Check zeigt, dass es bei einigen öffentlichen Stellen noch immer an den erforderlichen Grundkenntnissen zum Datenschutz und an der gebotenen Sensibilität im Umgang mit personenbezogenen Daten mangelt. Eine Erhebung personenbezogener Daten ohne Rechtsgrundlage und ohne bewusste Mitwirkung der Betroffenen stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar.

5.25 Nachweis einer Amtspflichtverletzung: TLfDI stößt an Grenzen bei sich widersprechenden Aussagen

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass die Bürgermeisterin einer Thüringischen Gemeinde nach einer Versammlung vor dem Verwaltungsgebäude vor einem größeren Kreis zufällig anwesender Personen ein Schreiben der Vollstreckungsstelle an eine Schuldnerin der Gemeinde vernehmbar verlesen habe.

Da insofern ein Verstoß gegen amtsbezogene Geheimhaltungspflichten sowie datenschutzrechtliche Bestimmungen nicht ausgeschlossen werden konnte, konfrontierte der TLfDI die Bürgermeisterin mit dem o. g. Beschwerdegegenstand.
Hierzu teilte die Bürgermeisterin mit, dass sie zwar nach der Versammlung vor dem Verwaltungsgebäude noch einige Minuten mit Gemeinderäten zusammengestanden habe. Dabei habe sie jedoch weder ein amtliches Schreiben verlesen noch personenbezogene Daten im Zusammenhang mit einer Vollstreckungsangelegenheit offenbart.
Der TLfDI wies den Beschwerdeführer in diesem Zusammenhang darauf hin, dass ihm keine vergleichbaren gesetzlichen Befugnisse zur exakten Klärung des realen Sachverhalts, wie etwa einer Staatsanwaltschaft, zur Verfügung stünden. Beurteilungsprobleme ergeben sich für den TLfDI insbesondere dann, wenn zwei plausible, sich jedoch widersprechende Sachverhalte vorgetragen werden und weitere Recherchen keine Aussicht auf Erfolg bieten. Dem TLfDI stehen auch in so einem Fall „nur“ ein Auskunfts- und Fragerecht gegenüber den öffentlichen Stellen und ein Einsichtsrecht in Akten und Dateien gemäß § 38 Abs. 1 Satz 2 Nr. 1 ThürDSG sowie ein Zutrittsrecht zu allen Diensträumen der öffentlichen Stellen gemäß § 38 Abs. 1 Satz 2 Nr. 2 ThürDSG zur Verfügung.
Leider war es auch in diesem Falle mit den Mitteln, die dem TLfDI zu Gebote stehen, ausgeschlossen, zweifelsfrei festzustellen, ob die Bürgermeisterin personenbezogene Daten im Zusammenhang mit einer Vollstreckungsangelegenheit offenbart hat. Da von der Beantwortung dieser Frage jedoch die datenschutzrechtliche Beurteilung der konkreten Angelegenheit entscheidend abhing, war die Angelegenheit für den TLfDI nicht weiter aufklärbar.

Leider sieht sich der TLfDI manchmal außerstande, mit den ihm zu Gebote stehenden Befugnissen Beschwerdesachverhalte exakt aufzuklären. Solche Schwierigkeiten ergeben sich insbesondere dann, wenn zwei plausible, sich jedoch widersprechende Sachverhalte vorgetragen werden und weitere Recherchen durch den TLfDI keine Aussicht auf Erfolg bieten. In diesem Fall nützen dem TLfDI weder sein Auskunfts- und Fragerecht, sein Akten- und Dateieneinsichtsrecht noch sein Zutrittsrecht zu allen Diensträumen gemäß § 38 Abs. 1 Satz 2 Nr. 1 und Nr. 2 ThürDSG.

5.26 Halter – Fahrer – Ehegatte – Familienangehörige: Wann ist der Abgleich mit dem Blitzer-Foto unzulässig?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte über folgenden Beschwerdesachverhalt Kenntnis:
Das Bürgeramt Erfurt habe die Ehefrau des Beschwerdeführers als verantwortliche Fahrerin für eine Geschwindigkeitsüberschreitung ermittelt, da deren Daten samt Lichtbild aus einem vorherigen Verfahren mit demselben Fahrzeug vorgelegen hätten. Der Halter des Fahrzeugs sei der Schwiegervater der Fahrerin.
Der Beschwerdeführer bat den TLfDI deshalb, mitzuteilen, ob und inwieweit die Identität des Fahrers bzw. der Fahrerin mittels Lichtbildabgleich – auch von mit im Haushalt eines Fahrzeughalters lebenden Angehörigen – durch Einsichtnahme in das Personalausweisregister ermittelt werden dürfe.
Wie die Stadtverwaltung Erfurt zunächst auf Anfrage des TLfDI mitteilte, habe aufgrund einer Recherche im EDV-Verfahren SCOWI und dem augenscheinlichen Alter der Fahrerin der Verdacht bestanden, dass sie, die Ehefrau des Beschwerdeführers, auch im aktuellen Verfahren das Kfz gefahren haben könnte. Um dies abzuklären, sei daraufhin ein Passbildabgleich gemäß § 24 Personalausweisgesetz (PAuswG) durchgeführt worden. Von einer Vorortermittlung durch den Außendienst sei gemäß § 24 Abs. 2 Nr. 3 PAuswG abgesehen worden, da der damit verbundene Aufwand gegenüber der Recherche im Personalausweisregister zu hoch sei.
Die Frage, die sich für den TLfDI stellte, war nun, zu prüfen, unter welchen Voraussetzungen ein solcher Lichtbildabgleich in Thüringen zulässig ist. Dabei stieß der TLfDI auf die Nummer 2.3.2 der Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei (VwV VAStVOWi) vom 19. Dezember 2006 (ThürStAnz. 2007, S. 171), der die Modalitäten des Lichtbilderabgleichs mit Passfotos aus dem Personalausweis bzw. Passregister zur Verfolgung von Verkehrsordnungswidrigkeiten regelt. Zur Auslegung dieser Regelung teilte das ehemalige Thüringer Innenministerium (TIM) dem TLfDI im Oktober 2014 u. a. Folgendes mit:

„Danach kommt die Anforderung von Lichtbildern bei den Meldebehörden erst nach Anhörung des Fahrzeughalters in Betracht. Dabei

*dürfen **nur Lichtbilder des Fahrzeughalters oder seines Ehegatten** angefordert werden. Die Anforderung von Lichtbildern anderer Haushaltsangehöriger ist nach der vorgenannten Verwaltungsvorschrift nicht zulässig."*

Im Beschwerdefall hätte somit nur das Lichtbild des Fahrzeughalters bzw. von dessen Ehefrau, nicht jedoch das Lichtbild der Schwiegertochter angefordert werden dürfen.
Aufgrund der o. g. Auslegung der Verwaltungsvorschrift VwV VA-StVOWi bat der TLfDI die Stadtverwaltung, zur Zulässigkeit des Lichtbilderabgleichs mittels des Personalausweisregisters im konkreten Fall sowohl rechtlich als auch tatsächlich Stellung zu nehmen. Die Stadtverwaltung legte sodann dem TLfDI dar, dass es sich aus ihrer Sicht beim Beschwerdeführer um einen von der Eintragung im Fahrzeugregister abweichenden Kfz-Halter im Sinne des Beschlusses des OLG Schleswig-Holstein vom 20. September 2004, 2 Ss 133/04 gehandelt habe. Nach diesem Beschluss sei derjenige als Halter anzusehen, der die Kosten bestreitet und tatsächlich über die Fahrzeugnutzung verfügen könne.
Vom TLfDI zu dieser Sachverhaltsauslegung durch die Stadtverwaltung Erfurt befragt, erklärte der Beschwerdeführer, dass er zwar das Kfz genutzt habe, jedoch sein Vater, der Kfz-Halter, die Kosten für das Fahrzeug tragen würde.
Wie weitere Recherchen des TLfDI ergaben, lagen der Stadtverwaltung Erfurt keine nachvollziehbaren Anhaltspunkte dafür vor, dass es sich beim Beschwerdeführer um einen von der Eintragung im Fahrzeugregister abweichenden Kfz-Halter im Sinne des genannten Beschlusses des OLG Schleswig-Holstein vom 20. September 2004 gehandelt hatte.
Somit erfolgte der Lichtbildabgleich des Blitzerfotos mit der Abbildung der Ehefrau des Beschwerdeführers durch die Stadt Erfurt entgegen der Nummer 2.3.2 der Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei (VwV VAStVOWi) vom 19. Dezember 2006 (Thür. Staatsanzeiger 2007, S. 171).

Im Ergebnis hat der TLfDI die o. g. unzulässige Datenerhebung der Stadt Erfurt gemäß § 39 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet und die Stadt Erfurt aufgefordert, künftig die Regelungen der Verwaltungsvorschrift zur Verfolgung und Ahn-

dung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und die Polizei (VwV VAStVOWi) vom 12. Juni 2006 in ähnlichen Fällen zu beachten.

Verantwortliche Stellen sind verpflichtet, die rechtlichen Regelungen zur Datenerhebung auch im Falle von Verkehrsordnungswidrigkeiten genau zu beachten. Gem. Nummer 2.3.2 der Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei (VwV VAStVOWi) vom 19. Dezember 2006 (Thür. Staatsanzeiger 2007, S. 171) ist ein Lichtbildabgleich nur für den Fahrzeughalter und seinen Ehegatten zulässig. Die Anforderung von Lichtbildern anderer Haushaltsangehöriger ist nach dieser Verwaltungsvorschrift nicht zulässig.

5.27 Rechtswidrige Datenübermittlung - der geblitzte künftige MP?

Am 17. April 2014 um 9:38 Uhr erfasste die Blitzer-Säule an der Bundesstraße 7 bei Weimar ein zu schnell fahrendes Auto mit dem amtlichen Kennzeichen EF-… . Dieser Sachverhalt, der in Deutschland jeden Tag tausendfach geschieht, wäre für eine Zeitung eigentlich uninteressant. In diesem Fall stand der mutmaßliche Fahrer aber wegen der Landtagswahl 2014 im Rampenlicht der Presse.
Am 6. November 2014 veröffentlichte die Bild-Zeitung in diesem Zusammenhang unter der Überschrift „Wird hier Thüringens neuer Landeschef geblitzt?“ einen Artikel mit Bildern. Auf einem dieser Bilder, einem so genannten Radarbild, soll der Vorsitzende der Fraktion DIE LINKE im Thüringer Landtag, Bodo Ramelow, zu erkennen gewesen sein.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm in der Folge Ermittlungen zum geschilderten Sachverhalt auf, weil der Verdacht im Raum stand, dass das in der Bild-Zeitung veröffentlichte Blitzerfoto aus der Verfahrensakte stammen könnte. Eine solche Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs ist nur unter den engen Voraussetzungen von § 22 ThürDSG zulässig. Deshalb stand hier eine unzulässige Datenübermittlung im Raum.
Im Zuge der Ermittlungen führte der TLfDI Kontrollen bei der Stadtverwaltung Weimar sowie bei der Staatsanwaltschaft Erfurt

durch. Gleichzeitig wurde die Direktorin des Amtsgerichtes Weimar zu diesem Sachverhalt befragt.
Trotz umfangreicher und mehrfacher Untersuchungen konnte der TLfDI im Ergebnis keine verwertbaren Beweise für ein Fehlverhalten der genannten öffentlichen Stellen feststellen, das zur Übermittlung der personenbezogenen Daten des Fahrers – hier also des Fotos – geführt hatte.
Indizien dafür, dass ein(e) infrage kommende(r) MitarbeiterIn der Stadtverwaltung Weimar die entsprechenden Fotos einer dritten Person übermittelt haben könnte, konnte der TLfDI nicht erhärten.
Anlässlich seiner Ermittlungen stellte der TLfDI jedoch fest, dass insgesamt 17 Personen bei der Stadtverwaltung Weimar zugriffsberechtigte Nutzer der dazugehörigen elektronischen Akte waren. Nach § 9 Abs. 2 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) ist zu gewährleisten, dass in jedem Falle nur die befugten Personen personenbezogene Daten in Ordnungswidrigkeitenverfahren zur Kenntnis nehmen können, damit die Vertraulichkeit gewahrt ist. In diesem Zusammenhang empfahl der TLfDI der Stadtverwaltung Weimar dringend, den Kreis der Zugriffsberechtigten, insbesondere zur elektronischen Akte, zu beschränken.
Ebenfalls konnte der TLfDI letztlich nicht aufklären, ob und wie gegebenenfalls Mitarbeiterinnen oder Mitarbeiter der Staatsanwaltschaft Erfurt für die Übermittlung des Lichtbildes verantwortlich waren.
Auch die Nachfrage bei der Direktorin des Amtsgerichtes Weimar hat keine Anhaltspunkte dafür ergeben, dass Bedienstete des Gerichtes das fragliche Foto des Fahrers einem Dritten übermittelt haben könnten.
Letztlich konnte der TLfDI somit nicht belastbar ermitteln, wer das Blitzerfoto an die Bild-Zeitung oder einen Dritten übermittelt hatte.

Die Übermittlung eines Blitzerfotos außerhalb des öffentlichen Bereichs ist nur unter den engen Voraussetzungen von § 22 ThürDSG zulässig. Sie kann unter den Voraussetzungen des § 43 Abs. 1 und 2 ThürDSG ordnungswidrig sein und deshalb mit Geldbuße bis zu 50.000 Euro geahndet werden. Ferner ist ein Straftatbestand nach § 43 Abs. 3 ThürDSG unter anderem dann verwirklicht, wenn der Täter sich das Foto aus einer nicht offenkundigen Datei verschafft und er ferner in Schädigungs- oder Bereicherungsabsicht gehandelt

hat. Dieses Vergehen kann mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe geahndet werden.

5.28 Geblitzt – wer darf Daten auswerten?

Die Stadt Erfurt wandte sich mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob für die stationäre Geschwindigkeitsüberwachung in der Landeshauptstadt Erfurt durch einen externen Auftragnehmer ein Vertragsverhältnis zur Datenverarbeitung im Auftrag nach der Mustervereinbarung gemäß dem 5. Tätigkeitsbericht des TLfDI, Anlage 23, geschlossen werden muss. Für die Beantwortung dieser Frage ist entscheidend, ob es sich um eine Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG) handelt. Das setzt voraus, dass die Stadt Erfurt weiterhin für die Verarbeitung und deren Ergebnisse verantwortlich bleibt und keine umfassende Funktionsübertragung an die externe Firma vorliegt. Eine Funktionsübertragung wäre nur durch oder aufgrund Gesetzes möglich. Da ein solches Gesetz nicht vorliegt, wäre die Datenerhebung durch die externe Firma unzulässig.
Auf Nachfrage des TLfDI teilte die Stadt Erfurt mit, dass im Rahmen der Dienstleistungen des Auftragnehmers die an den Messstationen entstandenen Daten zur amtlichen Kontrollauswertung durch die Behörde aufbereitet werden. Die Datenauswertung und -verarbeitung wird ausschließlich von der Stadt Erfurt vorgenommen. Die Aufarbeitung besteht lediglich darin, dass der Auftragnehmer Bilder in der Totalansicht sowie Bildausschnitte vom Fahrer und Kennzeichen generiert. Es werden Datum und Uhrzeit der Aufnahme und die gemessene Geschwindigkeit des Fahrzeugs und das am Standort geltende Geschwindigkeitslimit dargestellt. Diese Daten werden der Behörde zum Abruf auf einem gesicherten Server des Anbieters bereitgestellt. Die Aufbereitung dient allein dazu, dass die Stadt Erfurt die Bilder einer rechtlichen Prüfung unterziehen kann. Damit bleibt weiterhin die Stadt Erfurt die datenschutzrechtlich verantwortliche Stelle, eine Funktionsübertragung an den Auftragnehmer liegt nicht vor. Es ist daher ein Vertrag zu schließen, der den Anforderungen des § 8 ThürDSG entspricht.
Die Stadt Erfurt legte dem TLfDI den Vertrag zur Auftragsdatenverarbeitung im Anschluss zur Prüfung vor. Der TLfDI stellte nach

datenschutzrechtlicher Prüfung fest, dass der Vertrag die Anforderungen des § 8 ThürDSG erfüllte.

Wenn eine öffentliche Stelle für die Wahrnehmung von bestimmten Aufgaben Dritte heranzieht, ist für die Frage, ob eine Auftragsdatenverarbeitung nach § 8 ThürDSG vorliegt, entscheidend, wer für die Verarbeitung und Nutzung der Daten verantwortlich sein soll. Wenn alle wesentlichen Entscheidungen vom Auftragnehmer getroffen werden, liegt keine Auftragsdatenverarbeitung, sondern eine Funktionsübertragung vor. In diesem Fall wäre der Auftraggeber die für die Datenverarbeitung verantwortliche Stelle. Eine Funktionsübertragung ist nur durch oder aufgrund Gesetzes möglich.

5.29 Personenbeziehbarkeit von Daten zu einem Stadtentwicklungskonzept

Eine Stadtverwaltung bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum um die Bewertung der von ihr vorgesehenen Datenübermittlung an ein privates Planungsbüro im Rahmen der Fortschreibung eines Stadtentwicklungskonzeptes. Konkret begehrte das Planungsbüro unter anderem gebäudedifferenzierte Daten zur Altersstruktur, zur Stellung der Einwohner der Kommune im Erwerbsleben, zur Verkehrsmittelverfügbarkeit, zu Verkehrsmitteln und Verkehrszielen.
Zu diesem Vorhaben äußerte der TLfDI seine datenschutzrechtlichen Bedenken. Diese beruhten insbesondere darauf, dass bei der Erhebung der Verkehrsquellen bzw. -ziele eine adressscharfe Auflistung der Firmen mit konkreten Angaben über die jeweiligen Zufahrten und ihre Lieferanten und Kunden sowie der Anzahl der jeweils Beschäftigten gefordert wurde.
Da sich aus diesen Daten relativ leicht Personenbezüge ableiten ließen, schlug der TLfDI vor, die Einzelangaben nach Straßenabschnitten zusammenzufassen und die Anzahl der Beschäftigten und die Lieferanten und Kunden nicht als konkreten Wert, sondern in Form einer Von-bis-Spanne, zu übermitteln. Die Stadt Suhl hat den Vorschlag des TLfDI berücksichtigt und die o. g. Daten nur in der empfohlenen Form an das Planungsbüro übermittelt.

Bereits in der Entwurfsphase von Entwicklungskonzepten, Studien und Verfahren sollten datenschutzrechtliche Grundsätze wie Datensparsamkeit (§ 1 Abs. 2 Satz 1 ThürDSG), Anonymisierung und Pseudonymisierung (§ 1 Abs. 2 Satz 2 ThürDSG) sowie minimale Personenbeziehbarkeit beachtet werden.

5.30 Rathaus-Videokamera: dieses Mal nicht so gaga!

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) anonym über eine Videokamera am Rathaus Geschwenda in Kenntnis, wobei er sich darüber beschwerte, dass kein optischer Hinweis auf den Umstand der Überwachungsmaßnahme existiere.
Nachfolgend bat der TLfDI die Gemeindeverwaltung Geschwenda, zu der Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, auf welcher Rechtsgrundlage die Videoüberwachung beruhe und zu welchem Zwecke sie erfolge. Weiterhin forderte der TLfDI, ihn über die konkreten technisch-organisatorischen Regelungen zum Betrieb der Videoanlage in Kenntnis zu setzen (unter Berücksichtigung der unter Gliederungspunkt 5.2 ab S. 35 ff. des achten TLfDI-Tätigkeitsberichts aufgelisteten Kriterien zum Betrieb kommunaler Videoanlagen). Dazu forderte der TLfDI die entsprechenden Unterlagen, z. B. in Form einer Dienstanweisung, an.
Die Gemeindeverwaltung Geschwenda antwortete dem TLfDI, dass sie die Videoüberwachung zur Vermeidung von Beschädigungen am Rathaus und der angrenzenden Bushaltestelle installiert habe. Es seien von ihr mehrere Hinweisschilder auf die Videoüberwachung angebracht worden. Da es in den vergangenen Jahren mehrfach zu Randalen im Ort gekommen sei und die Gemeinde die im Rahmen der Dorferneuerung geschaffenen Werte erhalten wolle, sei die Installation einer Videoüberwachung erforderlich gewesen. Die Notwendigkeit des Betreibens der Anlage prüfe die Gemeinde zweimal im Jahr. Die von der Gemeindeverwaltung Geschwenda vorgelegte Dienstanweisung zum Einsatz von Videotechnik entsprach den datenschutzrechtlichen Vorgaben, insbesondere denen des § 25a Thüringer Datenschutzgesetz (ThürDSG). Im Ergebnis hatte der TLfDI daher keine Einwände gegen die geschilderte Videoüberwachung. Dies ergab sich auch daraus, dass der Bürger, der den TLfDI über die Videoüberwachung in Kenntnis gesetzt hatte, selbst keine eigene Beeinträchtigung seiner schutzwürdigen Interessen geltend gemacht

hatte, und eine solche auch nach Prüfung durch den TLfDI nicht vorlag.

Die Videoüberwachung mithilfe optisch-elektronischer Einrichtungen ist gemäß § 25a ThürDSG zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ferner prüft der TLfDI eine erforderliche Dienstanweisung zur Videoüberwachung anhand der Kriterien, die er unter dem Gliederungspunkt 5.2 auf den Seiten 35 ff. seines achten Tätigkeitsberichts veröffentlicht hat.

5.31 Videogaga 2 in Piesau

Ein Beschwerdeführer setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber in Kenntnis, dass am Gemeindeamt Piesau und am Treffpunkt der Gemeindejugend im Bauhof der Gemeinde Piesau je eine Videokamera installiert sei.
Der TLfDI wies die Bürgermeisterin von Piesau in diesem Zusammenhang auf die Regelung des § 25a Thüringer Datenschutzgesetz (ThürDSG) hin und bat sie, zu der Angelegenheit Stellung zu nehmen. Dabei interessierte den TLfDI, auf welcher Rechtsgrundlage die o. g. Videoüberwachungen beruhten und zu welchem Zwecke sie erfolgten. Zugleich forderte der TLfDI die Bürgermeisterin auf, ihn über die konkreten technisch-organisatorischen Regelungen der Gemeinde Piesau zum Betrieb der beiden Videokameras in Kenntnis zu setzen und entsprechende Unterlagen, z. B. in Form einer Dienstanweisung, zu übersenden. Der TLfDI verwies dabei auf die unter Gliederungspunkt 5.2 (Seiten 35 ff.) seines achten Tätigkeitsberichts aufgelisteten Kriterien zum Betrieb kommunaler Videoanlagen.
Daraufhin informierte die Bürgermeisterin den TLfDI darüber, dass beide o. g. Videokameras schon seit längerem defekt und außer Betrieb seien.
Zu diesem neuen Sachverhalt nahm der TLfDI gegenüber der Bürgermeisterin von Piesau wie folgt Stellung:
Auch deaktivierte Kameras können ebenso wie Kameraattrappen bei Passanten bzw. Besuchern den Anschein erwecken, dass ihr Verhalten überwacht werde. Dies könne eine negative Beeinflussung des

Verhaltens von Bürgern zur Folge haben. Somit sei die Angelegenheit gemäß § 25a ThürDSG zu beurteilen.
Im Ergebnis ging der TLfDI von einer datenschutzrechtlichen Unzulässigkeit der Installation der (deaktivierten) Videokameras bzw. Kameraattrappen aus, da Betroffene davon ausgehen konnten, dass sie mit derart platzierten Kameras aufgenommen werden.
Der TLfDI forderte die Bürgermeisterin von Piesau auf, beide Videokameras abzubauen bzw. sie mittels einer Schutzfolie erkennbar zu deaktivieren und ihn über den Vollzug dieser Maßnahmen in Kenntnis zu setzen.
Nachfolgend informierte die Bürgermeisterin von Piesau den TLfDI darüber, dass die defekten Kameras am Gemeindeamt und am Treffpunkt der Gemeindejugend mit einer Schutzfolie abgedeckt worden und damit nicht mehr sichtbar seien.

Da Kameraattrappen bzw. defekte Videokameras den Anschein einer Überwachung erwecken, ist demzufolge § 25a ThürDSG der Bewertungsmaßstab. Kameraattrappen bzw. defekte Kameras, die unzulässig sind, sind von der öffentlichen Stelle abzubauen bzw. abzudecken.

5.32 „Brennende“ Datenschutzprobleme bei der Auftragsdatenverarbeitung – Zur Notwendigkeit eines Auftragsdatenverarbeitungsvertrages

Die Stadtverwaltung Jena legte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum Unterlagen zur Software zum vorbeugenden Brandschutz (VoBraWeb) zur Bewertung vor. Die Stadtverwaltung beabsichtigte, der verantwortlichen Softwarefirma einen Auftrag zu erteilen. Jedoch vertrat die Softwarefirma zunächst die Auffassung, dass hierbei ein Vertrag über eine Auftragsdatenverarbeitung im Sinne des § 8 Thüringer Datenschutzgesetz (ThürDSG) nicht abgeschlossen werden müsste.
Der TLfDI stellte nach datenschutzrechtlicher Prüfung fest, dass im o. g. Verfahren personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG, z. B. Name, Adresse und Telefonnummer von Hauseigentümern als Kontaktdaten, verarbeitet und genutzt wurden. Unerheblich war dabei, ob diese Daten anderweitig öffentlich zugänglich waren. Bei dem Verfahren VoBraWeb stellt die Soft-

warefirma im Rahmen des Geschäftsmodells „Software as a Service (SaaS)“ neben der Software auch ein Serversystem zur Speicherung der Kundendaten zur Verfügung. Die Speicherung ist gemäß § 3 Abs. 3 Nr. 2 ThürDSG vom Begriff der Datenverarbeitung umfasst.

Im Ergebnis handelte es sich bei der beabsichtigten Geschäftsbeziehung zwischen der Stadtverwaltung und der Softwarefirma deshalb um eine Verarbeitung personenbezogener Daten im Auftrag, die eines Vertrages gemäß § 8 ThürDSG bedurfte.

In diesem Zusammenhang empfahl der TLfDI der Stadtverwaltung den Mustervertrag zur Auftragsdatenverarbeitung aus dem 5. Tätigkeitsbericht des TLfDI, Anlage 23. Der TLfDI stellte klar, dass der Auftraggeber für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz dann verantwortlich bleibt, wenn personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt werden, § 8 i. V. m. § 9 ThürDSG.

In dem vom TLfDI zu prüfenden Sachverhalt war ferner zu berücksichtigen, dass bei dem Geschäftsmodell SaaS die Anwender i. d. R. regelmäßig keinen direkten administrativen, operativen oder kontrollierenden Zugriff haben. Insoweit stellte sich für den TLfDI die Frage, wie die Stadtverwaltung prüfen kann, ob der Anbieter auch hinreichende Garantien für die Sicherheit und Ordnungsmäßigkeit aller bereitgestellten Ressourcen anbot und ob das Anwendungsverfahren hinsichtlich der Nutzung personenbezogener Daten den für die Stadtverwaltung geltenden gesetzlichen Bestimmungen genügte. In jedem Fall, so der Rat des TLfDI, sollte sich die Stadtverwaltung die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig darlegen lassen und vor Vertragsunterzeichnung prüfen (§ 8 Abs. 2 Satz 1 ThürDSG)

Weitere Ausführungen zu dieser Problematik finden sich in der Orientierungshilfe Cloud-Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

(http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/orientierungshilfe_cloud_computing.pdf).

Der TLfDI wies die Stadtverwaltung ausdrücklich darauf hin, dass der Auftrag nicht

an die Softwarefirma zu erteilen sei, falls das Unternehmen den Abschluss eines solchen Vertrages gemäß § 8 ThürDSG ablehnen sollte.
Letztendlich legte die Stadtverwaltung Jena dem TLfDI einen sowohl von ihr als auch der Softwarefirma unterschriebenen datenschutzkonformen Vertrag zur Auftragsdatenverarbeitung vor.

In der Regel bedarf auch eine Geschäftsbeziehung im Rahmen des Geschäftsmodels „Software as a Service“ eines Vertrages zur Auftragsdatenverarbeitung nach § 8 ThürDSG. Verweigert die Softwarefirma den Abschluss eines solchen Vertrages, so darf die öffentliche Stelle den Auftrag nicht erteilen.

5.33 Offene Unterstützungslisten bei der Kommunalwahl

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die Unterstützungslisten von Kandidaten der Kommunalwahlen, die in der Stadtverwaltung geführt werden, mit den darin enthaltenen personenbezogen Daten der Unterstützer für denjenigen sichtbar seien, der vorgebe, sich in der betreffenden Unterstützungsliste eintragen zu wollen.
Hierzu teilte der TLfDI mit, dass nach § 14 Abs. 6 Satz 1 und 2 Thüringer Kommunalwahlgesetz Wahlberechtigte, die einen Wahlvorschlag unterstützen wollen, sich in den bei der Gemeinde ausgelegten Unterstützungslisten unter Angabe ihres Vor- und Nachnamens, ihrer Anschrift und ihres Geburtsdatums einzutragen und eine eigenhändige Unterschrift zu leisten haben.
Mit Schreiben vom 24. März 2014 hatte sich das frühere Thüringer Innenministerium (TIM) gegenüber dem Thüringer Landesverwaltungsamt, den Landkreisen, Gemeinden, Verwaltungsgemeinschaften und Wahlleitern zu der o. g. Thematik wie folgt geäußert:
„Der Wahlvorschlag ist vom Tag nach der Einreichung verbunden mit einer Liste zur Leistung von Unterstützungsunterschriften während der üblichen Dienstzeiten der Gemeindeverwaltung zur Unterschriftsleistung auszulegen. Aus Datenschutzgründen ist darauf zu achten, dass die Unterschriftsleistenden nicht die bereits geleisteten Unterschriften einsehen (z. B. durch Abdecken); auch Beauftragte des Wahlvorschlags haben kein Einsichtsrecht.“

Abschließend teilte der TLfDI dem Beschwerdeführer mit, dass die Angelegenheit momentan als erledigt anzusehen sei, da dafür Sorge getragen wurde, dass die Unterschriftsleistenden nicht die bereits geleisteten Unterschriften einsehen konnten. Natürlich wäre es noch datenschutzgerechter, wenn die o. g. Verfahrensweise der Unterschriftsleistung und der Schutz vor Einsichtnahme gesetzlich geregelt wären. Der TLfDI wird dies im Rahmen einer künftigen Novellierung des Thüringer Kommunalwahlgesetzes anregen.

Im Rahmen einer künftigen Novellierung des Thüringer Kommunalwahlgesetzes sollte auch die „Datenschutzlücke“ der unbefugten Einsichtnahme in Unterstützerlisten zur Kommunalwahl geschlossen werden.

5.34 Widerspruch zum Widerspruch – auf das Widerspruchsrecht muss angemessen hingewiesen werden

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Information, dass die Stadt Jena ein Baulandkataster mit Grundstücken einer bestimmten Mindestgröße, die als potenzielles Bauland in Betracht kamen, erstellt und öffentlich zugänglich gemacht hätte. Bedenklich erschien hierbei die Gestaltung der Widerspruchmöglichkeit der Grundstückseigentümer. Nach § 200 Abs. 3 Satz 2 und 3 Baugesetzbuch (BauGB) kann die Gemeinde die betreffenden Flächen veröffentlichen, soweit der Grundstückseigentümer nicht widersprochen hat. Die Gemeinde hat danach ferner ihre Absicht zur Veröffentlichung einen Monat vorher öffentlich bekannt zu geben und dabei auf das Widerspruchsrecht der Grundstückseigentümer hinzuweisen.
Die Stadt Jena hatte in ihrem Amtsblatt mitgeteilt, dass sie beabsichtige, frühestens nach Ablauf eines Monats, gerechnet ab der Bekanntgabe ihrer Veröffentlichungsabsicht, auf ihrer Internetseite ein Baulandkataster zu jedermanns Einsicht bereitzuhalten. Die Stadt führte weiter aus, dass im Fall von fristgerechten Widersprüchen die betroffenen Grundstücke aus dem Baulandkataster entfernt würden. Ein zusätzlicher Passus besagte, dass „… *nach Fristablauf eingehende Widersprüche nur insoweit Berücksichtigung finden, als dass eine nachträgliche Streichung der Angaben ohne unverhältnismäßigen Aufwand möglich ist*.“ Eine dem kursiv gekennzeichneten Wort-

laut entsprechende Mitteilung befand sich auch in einem Anschreiben der Stadt Jena an die betroffenen Grundstückseigentümer.
Die Stadt teilte erst auf Nachfrage des TLfDI mit, dass sich der o. g. kursiv gekennzeichnete Wortlaut ausschließlich auf nicht-digitale Formen des Baulandkatasters bezöge, wobei Bürger gedruckte Karten mit den Baulandkatasterflächen in der Stadtverwaltung einsehen könnten. Laut der Aussage der Stadt Jena hätte es einen unverhältnismäßigen Aufwand bedeutet, diese Karten nach jedem einzelnen Widerspruch neu zu drucken.
Das Anschreiben der Stadt Jena an die betroffenen Grundstückseigentümer enthielt die Anlage „*Information: Fragen und Antworten*“, das auch als PDF-Dokument auf der Internetseite der Stadt Jena abrufbar war. Darin enthalten war der Hinweis: „*Wurde Ihr Grundstück bereits im Baulandkataster veröffentlicht, so können Sie auch zu einem späteren Zeitpunkt der Veröffentlichung widersprechen. Das in Ihrem Eigentum befindliche Grundstück wird zum nächstmöglichen Zeitpunkt aus der im Internet veröffentlichten Datenerfassung entfernt*.“
Aus dem Wortlaut des Amtsblattes, dass die nach Fristablauf eingehenden Widersprüche nur berücksichtigt würden, wenn deren Umsetzung keinen unverhältnismäßigen Aufwand erfordere, entstand der Eindruck, dass die Stadt Jena nicht alle Widersprüche bearbeiten werde. Zudem enthielt das Amtsblatt keinen Hinweis dazu, dass sich diese genannte Einschränkung nur auf nicht-digitale Formen des Baulandkatasters in Form von gedruckten Karten bezog. Die Formulierung im Amtsblatt, wonach Eigentümer mittels eines unter einer angegebenen Internetadresse abrufbaren Formulars auch nach der Veröffentlichung des Katasters von ihrem Widerspruchsrecht Gebrauch machen könnten, ließ zudem einen Hinweis darüber vermissen, dass auch schriftliche Widersprüche, bei denen das Formular nicht benutzt wurde, jederzeit von der Stadt Jena bearbeitet werden.
Zusammenfassend stellte der TLfDI fest, dass die Informationen zum Widerspruchsrecht unvollständig waren, sich teilweise widersprachen und somit für den Bürger irritierend sein konnten. Einzig die „Information: Fragen und Antworten“ entsprach – für sich genommen –den Vorgaben des § 200 Abs. 3 Satz 2 und 3 BauGB, wonach ein Grundstückseigentümer der Veröffentlichung hinsichtlich der ihn und sein Grundstück betreffenden Angaben jederzeit auch nach Ablauf der Monatsfrist widersprechen kann (Battis/Krautzberger/Löhr, BauGB-Kommentar, 12. Auflage, Anm. 9 zu

§ 200, S. 1512 und inhaltsgleich BauGB-Kommentar, 7. Auflage, W. Schröder, Anm. 8, S. 1958).
Der TLfDI bat die Stadt um Mitteilung, welche Maßnahmen sie zur Herstellung einer umfassenden und widerspruchsfreien Information der Betroffenen zur Wahrnehmung des Widerspruchsrechts zum Baulandkataster beabsichtige. Der TLfDI selbst schlug vor, eine klarstellende Presseerklärung zu veröffentlichen oder ein entsprechendes Anschreiben zu erstellen. Die Stadt Jena folgte dem Hinweis des TLfDI und teilte ihm daher mit, eine entsprechende Pressemitteilung vorzubereiten.

Datenschutzrechtliche Transparenz ist im „Bürokraten-Dschungel" nicht immer leicht herzustellen: Im Fall der Stadt Jena mangelte es den von der Stadt veröffentlichten Hinweisen zum Widerspruchsrecht an der in datenschutzrechtlicher Hinsicht gebotenen Klarheit, wodurch die Ausübung des informationellen Selbstbestimmungsrechts der betroffenen Grundeigentümer in Form der Geltendmachung eines Widerspruchrechts nach § 200 Abs. 3 Satz 2 und Satz 3 Baugesetzbuch in unzulässiger Weise einschränkt wurde. Die Einschaltung des TLfDI brachte hier am Ende hinreichende Klarheit.

5.35 Der mitteilsame Oberbürgermeister – Vorsicht bei Pressemitteilungen

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis über einen Sachverhalt, der im Laufe seiner Kontrollpraxis der letzten Jahre als alles andere als datenschutzrechtlich „gewöhnlich" zu bezeichnen war.
Ein leitender Beamter der Stadt Nordhausen berichtete dem TLfDI, dass gegen ihn eine Staatsanwaltschaft ein strafrechtliches Ermittlungsverfahren wegen des Vorwurfs des sexuellen Missbrauchs widerstandsunfähiger Personen gemäß § 179 Abs. 5 Strafgesetzbuch geführt habe. Hauptbelastungszeugin sei eine Kollegin des Beamten und zugleich das mutmaßliche Opfer (so genannte Opferzeugin) gewesen. Ende September 2013 habe die zuständige Staatsanwaltschaft dieses Ermittlungsverfahren aber gemäß § 170 Abs. 2 Strafprozessordnung eingestellt. Der Grund dafür war, was die Recherchen des TLfDI bestätigten, dass die Staatsanwaltschaft keine Anhaltspunkte für ein dem beschuldigten Beamten vorgeworfenes Han-

deln nachweisen konnte. Die Staatsanwaltschaft hielt den Beamten deshalb für unschuldig, kommunizierte ihr Ermittlungsergebnis gegenüber der Presse und gab ansonsten keine weiteren Details ihres ermittelten Geschehensablaufs preis.

Dieses Ermittlungsergebnis der Staatsanwaltschaft kommentierte der Oberbürgermeister mit einer eigenen Pressemitteilung zu dieser Causa: Darin war unter anderem zu lesen, dass in dem genannten Ermittlungsverfahren „Aussage gegen Aussage" stehe. Ferner ließ der Oberbürgermeister darin vermelden, dass

„ *die Zeugenaussage der betroffenen ... [Hauptbelastungszeugin] ebenso glaubwürdig sei wie die nicht zu widerlegende Behauptung von ...[dem beschuldigten Beamten], es habe sich um einvernehmlichen Geschlechtsverkehr* ***unter Alkoholeinfluss*** *gehandelt*" (so die Pressemitteilung der Stadtverwaltung Nordhausen vom 27. September 2013, abgedruckt unter (http://www.nnz-online.de/news/news_lang_druck.php?ArtNr=135058).

Mit diesem Inhalt versandte der Oberbürgermeister seine Pressemitteilung an den Presseverteiler der Stadt. Dies hatte zur Folge, dass noch am selben Tag und zeitlich nach der Absendung der Pressemitteilung durch den Oberbürgermeister auf dem Internetportal „inSüdthüringen.de" Folgendes zu lesen war:

„*Zwischen… [dem Beamten und der Opferzeugin] soll es auf einer Dienstreise zum Sex gekommen sein. Der… [Beamte] hatte erklärt, es habe sich um einvernehmlichen Geschlechtsverkehr unter Alkoholeinfluss gehandelt*." (so die Meldung im Internetportal „InSüdthüringen.de" vom 27. September 2013 von 16:57 Uhr).

Der betroffene Beamte bat den TLfDI um datenschutzrechtliche Prüfung der Vorgehensweise des Oberbürgermeisters, in der Pressemitteilung zu verlautbaren, dass es im Ermittlungsverfahren der Staatsanwaltschaft um einen Geschlechtsverkehr „unter Alkoholeinfluss" gegangen sei. Das Faktum „unter Alkoholeinfluss" sei weder von der Staatsanwaltschaft noch von ihm, dem Beamten selbst, in der Presse jemals genannt worden. Erst durch die Pressemitteilung des Oberbürgermeisters sei dieser Vorwurf in die Öffentlichkeit

gelangt. Die datenschutzrechtliche Prüfung durch den TLfDI ergab dabei Folgendes:
Bei den Informationen „Geschlechtsverkehr unter Alkoholeinfluss“ handelte es sich zunächst um Einzelangaben über persönliche Verhältnisse von bestimmbaren Personen und damit um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG. Denn sowohl bei der Information „Geschlechtsverkehr“ als auch bei der Information „unter Alkoholeinfluss“ werden geistige Zustände bzw. körperliche Merkmale genannt, die allesamt unter den Begriff der persönlichen Verhältnisse zu subsumieren sind (vgl. Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 3, Rz. 10). Diese persönlichen Verhältnisse waren auch auf den beschuldigten Beamten bzw. die Opferzeugin eindeutig beziehbar.
Indem die Stadtverwaltung Nordhausen die genannten beiden personenbezogenen Daten im unmittelbaren Kontext (Geschlechtsverkehr unter Alkoholeinfluss) in der Pressemitteilung erwähnte und diese per E-Mail an den Presseverteiler versandte, übermittelte sie diese auch im Sinne von § 3 Abs. 3 Nr. 4. a) ThürDSG.
Die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ durch die Pressemitteilung des Oberbürgermeisters erfolgte auch ohne Rechtsgrundlage. Denn weder war die Datenübermittlung durch § 22 Abs. 1 Nr. 1 ThürDSG noch durch § 22 Abs. 1 Nr. 2 ThürDSG gerechtfertigt.
§ 22 Abs. 1 Nr. 1 ThürDSG schied im vorliegenden Sachverhalt als Ermächtigungsgrundlage aus, weil die Übermittlung des genannten personenbezogenen Datums „unter Alkoholeinfluss“ zur Erfüllung der Aufgaben des Oberbürgermeisters nicht erforderlich gewesen ist.
Der Oberbürgermeister berief sich zwar darauf, dass er aus der „Fürsorgepflicht des Dienstherrn“ gehalten war, „unabgewogene(n) Pressemitteilungen“ und dem Eindruck entgegenzuwirken, dass die Opferzeugin „nachweislich gelogen habe“. Selbst wenn der TLfDI aber in dieser Frage unterstellt hätte, dass eine solch weitgehende Fürsorgepflicht des Dienstherrn tatsächlich existierte, so war es gleichwohl nicht erforderlich, dass der Oberbürgermeister quasi zur Wiederherstellung der Glaubwürdigkeit der Opferzeugin das personenbezogene Datum „unter Alkoholkonsum“ mit dem personenbezogenen Datum „Geschlechtsverkehr“ in einen unmittelbaren Kontext stellt und an die Presse übermittelt. Denn nach dem Grundsatz der Erforderlichkeit ist von mehreren geeigneten Maßnahmen diejenige zu wählen, die den einzelnen am wenigsten beeinträchtigt (siehe dazu Maurer,

Allgemeines Verwaltungsrecht, 17. Auflage, § 10, Rz. 17). Dafür hätte es ausgereicht, wenn der Oberbürgermeister allein darauf hingewiesen hätte, dass Aussage gegen Aussage stehe.
Auch § 22 Abs. 1 Nr. 2 ThürDSG konnte im vorliegenden Sachverhalt nicht als Rechtsgrundlage für die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ herangezogen werden. Denn ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hatte insbesondere der betroffene Beamte, aber auch die Opferzeugin.
Dieses bestand hier darin, die Öffentlichkeit nicht wissen zu lassen, dass es unter Alkoholeinfluss zwischen beiden zum Geschlechtsverkehr gekommen war. Denn bei dieser Information handelte es sich um ein – höchst persönliches – personenbezogenes Datum. Dieses personenbezogene Datum ist schützenswert im Sinne von § 22 Abs. 1 Nr. 2 ThürDSG, wenn es aus objektiver Sicht unter Zugrundelegung durchschnittlicher Verhältnisse zu Nachteilen für den Betroffenen führen kann (vgl. zur gleich lautenden Regelung in § 16 Abs. 1 Nr. 2 BDSG Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 16, Rz. 21). Welcher Art die drohenden Nachteile dabei sind, etwa wirtschaftlicher, sozialer oder persönlicher Art, ist dabei gleichgültig (vgl. auch insoweit, Dammann in Simitis, a.a.O., § 16, Rz. 22).
Vorliegend war der Nachteil für den betroffenen Beamten vor allem darin zu sehen, dass von ihm aufgrund der Pressemitteilung des Oberbürgermeisters das personenbezogene Datum des „Geschlechtsverkehrs unter Alkoholeinfluss“ in die Öffentlichkeit gelangte. Diese Information konnte seine Integrität, bzw. sein Ansehen beschädigen und damit zu sozialen und persönlichen Nachteilen führen.
Das Gleiche galt hier für die betroffene Opferzeugin. Zusätzlich war bei ihr an dieser Stelle zu berücksichtigen, dass durch Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ an die Presse der mit der Pressemitteilung des Oberbürgermeisters verfolgte Zweck, nämlich den Eindruck zu vermeiden, dass die Opferzeugin „nachweislich gelogen habe“, gerade nicht dienlich war und daher auch insoweit Nachteile persönlicher Art für die Opferzeugin zu befürchten waren.
Diese dargestellten schutzwürdigen Interessen des betroffenen Beamten und der betroffenen Opferzeugin wogen im Ergebnis auch höher als das Interesse der Pressevertreter, Detailkenntnisse über den Sachverhalt zu erfahren, der Gegenstand des strafrechtlichen Ermitt-

lungsverfahrens gegen den betroffenen Beamten war. Denn über die wesentlichen Gründe für die Einstellung des strafrechtlichen Ermittlungsverfahrens hatte der Pressesprecher der zuständigen Staatsanwaltschaft die Medien hinreichend unterrichtet.
Daran änderte auch der Einwand des Oberbürgermeisters nichts, dass sämtliche Presseartikel, die einen „Geschlechtsverkehr unter Alkoholeinfluss“ thematisiert hätten, zeitlich vor der Veröffentlichung der Pressemitteilung des Oberbürgermeisters erschienen seien.
Denn diese behauptete zeitliche Reihenfolge von Medienveröffentlichungen traf nach den Recherchen des TLfDI gerade nicht zu. Die vom Oberbürgermeister veröffentlichte Pressemitteilung war demnach am besagten Tag Ende September 2013 mindestens eineinhalb Stunden vor dem Erscheinen des Artikels im Portal „inSüdthüringen.de“ veröffentlicht worden. Dies konnte der TLfDI dem Oberbürgermeister anhand weiterer Presseveröffentlichungen an diesem Tage belegen.
Schließlich kam auch § 4 Abs. 1 Thüringer Pressegesetz (TPG) hier nicht als Ermächtigungsgrundlage für eine Datenübermittlung infrage. Dies ergab sich bereits aus § 4 Abs. 1 Satz 2 TPG. Danach steht in Thüringen einer Behörde gerade dann kein Ermessen hinsichtlich des presserechtlichen Auskunftsanspruchs zu, soweit Vorschriften über die Geheimhaltung und den Datenschutz entgegenstehen. In den genannten Fällen trifft die Behörde eine Pflicht zur Verschwiegenheit (so Weberling in: Ricker/Weberling, Handbuch des Presserechts, 6. Auflage, 4. Abschnitt, 20. Kapitel, Rz. 3; ebenso Löffler, Presserecht, 5. Auflage, Kommentar, § 4, Rz. 92). Eine solche Pflicht zur Verschwiegenheit traf im vorliegenden Fall auch den Oberbürgermeister, da ihn – wie dargelegt – die Regelungen von § 22 Abs. 1 Nr. 1 und Abs. 1 Nr. 2 ThürDSG an einer Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ an die Presse hinderten.
Aufgrund des Ergebnisses der datenschutzrechtlichen Prüfung beanstandete der TLfDI gemäß § 39 Abs. 1 Satz 1 ThürDSG die rechtswidrige Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ in Form der Pressemitteilung des Oberbürgermeisters.

Weder ein Bürger noch eine Behörde sollte sich im Zweifelsfall anmaßen, die „bessere“ Justizbehörde sein zu wollen. Denn das geht entweder juristisch schief oder verletzt sogar das Recht auf informationelle Selbstbestimmung Betroffener. Ein personenbezogenes Da-

tum aus einem ermittelten Sachverhalt ist daher entweder nur von der ermittelnden Behörde selbst oder gar nicht zu veröffentlichen. Sofern eine öffentliche Stelle doch meint, es „besser zu wissen", begeht sie einen Datenschutzverstoß gemäß § 39 Abs. 1 in Verbindung mit § 22 Abs. 1 Nr. 1 und Nr. 2 ThürDSG und wird deshalb vom TLfDI für ihr rechtswidriges Handeln beanstandet.

5.36 Eichsfelder Wurst oder Datenschutz bei Internetumfragen

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Internetumfrage unter dem Link http://www.dachmarke-eichsfeld.de/ zur Lebensqualität im Eichsfeld. Eine einheimische Softwarefirma habe die Umfrage im Auftrag des Landratsamts Eichsfeld durchgeführt.

Der TLfDI stellte im Rahmen seiner Recherchen fest, dass mittels o. g. Umfrage neben einer Vielzahl persönlicher Meinungen u. a. auch die religiöse Überzeugung des Teilnehmers der Umfrage abgefragt wurde. Der Teilnehmer hatte keine Möglichkeit, einzelne Fragen auszulassen. Daher blieb ihm nichts anderes übrig, als die Umfrage abzubrechen, wenn er bestimmte Fragen nicht beantworten wollte. Am Ende der Umfrage stellte die Softwarefirma allen Teilnehmern den Gewinn eines Wurstkorbs in Aussicht, wenn sie ihre E-Mail-Adresse mitteilten. Ein Hinweis auf die erforderliche Einwilligung in die beabsichtigte Verwendung der erhobenen personenbezogenen bzw. personenbeziehbaren Daten erfolgte dabei nicht.

Indem der Umfrageteilnehmer mit einem als Gewinn in Aussicht gestellten Wurstkorb „gelockt" werden sollte, seine E-Mail-Adresse, die als ein personenbezogenes Datum im Sinne von § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) anzusehen ist, preiszugeben, konnte auf diesem Wege ohne Weiteres nachvollzogen werden, welche religiösen Überzeugungen und sonstigen persönlichen Anschauungen der Betroffene vertritt. Bei Angaben zu religiösen Überzeugungen handelt es sich um besonders schutzwürdige Daten im Sinne von § 4 Abs. 5 ThürDSG.

Da anzunehmen war, dass der Softwarefirma ein Analysewerkzeug, z. B. zur örtlichen Selektion der Umfrageteilnehmer und ggf. zur

Auswertung ihres Nutzungsverhaltens zur Verfügung stand, konnte der TLfDI auch in diesem Zusammenhang die Erhebung weiterer personenbezogener Daten nicht ausschließen.
Das Betreiben der o. g. Webseite mit Eingabemöglichkeiten stellte zugleich einen Telemediendienst nach dem Telemediengesetz (TMG) dar. Die Anbieter für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien haben deshalb die unter § 5 Abs. 2 Nr. 1 bis 7 TMG angegebenen Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten (Impressumspflicht).
Ferner darf gemäß § 13 Abs. 2 Nr. 1 TMG eine solche Webseite nur betrieben werden, wenn der Nutzer gegenüber dem Webseitebetreiber in die damit verbundene Übertragung personenbezogener Daten bewusst und eindeutig eingewilligt hat. Da die Pflichtangaben gemäß § 5 TMG sowie die Einwilligungsaufforderung in die Datenübermittlung gemäß § 13 Abs. 2 TMG nicht festgestellt werden konnten, war ein Verstoß gegen das TMG in diesem Falle nicht auszuschließen.
Der TLfDI teilte dem Landratsamt Eichsfeld mit, dass im Zusammenhang mit der o. g. Webseite ein Verstoß gegen § 5 und § 13 Abs. 2 TMG seitens des beauftragten Softwareunternehmens nicht ausgeschlossen werden könne. Ferner forderte der TLfDI das Landratsamt auf, zu der Angelegenheit Stellung zu nehmen und den Vertrag zur Datenverarbeitung im Auftrag nach § 8 ThürDSG mit dem Softwareunternehmen vorzulegen, das die Internet-Umfrage durchgeführt hatte.
Daraufhin teilte das Landratsamt Eichsfeld dem TLfDI mit, dass es das Softwareunternehmen nur mit der strategischen Erarbeitung einer Dachmarken- und Standortmarketingkonzeption für das Eichsfeld beauftragt habe. Die Durchführung einer Internetumfrage sei von ihm nicht explizit gefordert worden. Vielmehr sollte es dem Auftragnehmer, hier also der Softwarefirma, überlassen bleiben, auf welche Art und Weise er den Ist-Zustand feststellt.
Entsprechende Nachweise legte das Landratsamt in Form einer Leistungsbeschreibung „Entwicklung einer Markenkonzeption und eines Corporate Designs für die Region Eichsfeld“ und eines nichtförmlichen und nicht näher konkretisierten Schreibens zur Auftragserteilung vor. Ferner, so das Landratsamt, sei mittlerweile die Internetumfrage beendet worden.
Abschließend regte der TLfDI gegenüber dem Landratsamt Eichsfeld an, künftig den Auftragnehmer in verbindlicher Form vorsorg-

lich auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen, wenn bei diesem die Umsetzung der allgemeinen vertraglichen Leistungsvorgaben eine Verarbeitung personenbezogener Daten erfordern sollte. Weiterhin wies der TLfDI darauf hin, dass § 8 ThürDSG explizit für öffentliche Stellen die Voraussetzungen und die Folgen der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag regelt.

Eine öffentliche Stelle hat den Auftragnehmer gerade dann auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen, wenn die Umsetzung allgemeiner vertraglicher Leistungsvorgaben eine Verarbeitung personenbezogener Daten beim Auftragnehmer erfordern sollte. Dies ergibt sich aus § 8 Thüringer Datenschutzgesetz, der die Verarbeitung oder Nutzung personenbezogener Daten im Auftrag regelt. Mehr Sensibilität in Sachen Datenschutz ist hier den öffentlichen Stellen zu empfehlen, auch wenn es sich im konkreten Fall um personenbezogene Daten handelte, die die Bürger selbst im Netz preisgaben.

5.37 Hundezensus

Die Stadt Gotha bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Beratung. Sie wollte in Erfahrung bringen, inwieweit es datenschutzrechtlich möglich wäre, dass die Stadt ein Unternehmen beauftragt, das in jedem Haushalt nachfragt, ob in diesem ein Hund gehalten werde. Nicht gemeldete Hunde könnten somit aufgespürt werden. Die Hundesteuersatzung der Stadt sah eine Hundebestandsaufnahme durch ein privates Unternehmen nicht vor.
Der TLfDI teilte der Stadt Gotha hierzu Folgendes mit:
Die Beauftragung eines privaten Unternehmens zwecks Wahrnehmung kommunaler Aufgaben wäre unter anderem dann möglich, wenn eine Rechtsgrundlage dies zuließe. Als solche käme eine kommunale Hundesteuersatzung grundsätzlich in Betracht. Allerdings bedürfte die Hundesteuersatzung in diesem Falle einer besonderen Regelung, wonach Grundstückseigentümer oder Haushaltsvorstände verpflichtet sind, den Mitarbeitern der Stadt bzw. den Mitarbeitern eines beauftragten Unternehmens, auf deren Nachfrage über die von ihnen gehaltenen Hunde und deren Halter wahrheitsgemäß Auskunft zu erteilen.

Unabhängig von einer entsprechenden Regelung in einer Satzung bestünde die Möglichkeit, dass Private auch ohne ausdrückliche gesetzliche Ermächtigung, nämlich in Form der Verwaltungshilfe an der Erfüllung von Aufgaben der öffentlichen Verwaltung beteiligt werden könnten. Sie würden dann weisungsabhängige Hilfstätigkeiten ohne eigene Entscheidungsbefugnis ausführen. Die Mitarbeiter dieser Unternehmen hätten in diesem Falle aber keine besonderen Befugnisse, beispielsweise die Grundstücke zu betreten, um dort nach Beweisen zu suchen, die auf eine Hundehaltung hinweisen könnten oder die Identität der dort lebenden Personen festzustellen. Sie müssten sich an die Weisungen der Stadt hinsichtlich des Befragungsumfangs und der sonstigen Umstände der Durchführung der Befragung halten. Die Stadt Gotha müsste dazu eine präzise Beschreibung dessen vornehmen, was und auf welche Weise etwas erfragt werden soll. Die Stadt müsste ferner festlegen, dass die Mitarbeiter des beauftragten Unternehmens den Weisungen der Gemeinde unterlägen und zur Verschwiegenheit verpflichtet wären. Die Tätigkeit des beauftragten Unternehmens müsste zudem durch die Stadt überwacht werden. Zu beachten wäre weiterhin, dass im Falle der Auftragsdatenverarbeitung das Steuergeheimnis gewahrt bliebe (§ 15 Abs. 1 Thüringer Kommunalabgabengesetz i. V. m. § 30 Abgabenordnung (AO)). Das Steuergeheimnis ist berührt, wenn Steuerdaten kommunaler Stellen von Dritten verarbeitet werden. Eine hierfür erforderliche bereichsspezifische Rechtsgrundlage ist weder den kommunalrechtlichen Vorschriften noch der AO oder dem Finanzverwaltungsgesetz (FVG) zu entnehmen. Daher dürften die beauftragten Unternehmen keine Vorabinformationen erhalten, wer bereits Hundesteuern zahlt.

Ende November 2015 wurde in der Stadt Gotha eine Änderung der Hundesteuersatzung beschlossen. In einem extra neu eingefügten Paragrafen der Satzung wurde festgelegt, dass die Verwaltung externe Unternehmen beauftragen kann, eine Hundebestandsaufnahme durchzuführen. Die Umsetzung dieser Regelung wird der TLfDI „im Auge behalten“.

5.38 Captain Chaos als Nächster bitte ... – Datenschutz bei elektronischen Anzeigetafeln

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum den Hinweis, dass die elektronische Anzeigetafel im Bürgerservice der Stadt Jena die Namen von Bürgern sichtbar anzeige. Die Namen könnten somit auch von den anderen Wartenden wahrgenommen werden.
Der TLfDI bat die Stadt Jena um Mitteilung, ob die Bürger wissen, dass ihre Namen auf der elektronischen Anzeigetafel angezeigt werden. Die Stadt Jena teilte daraufhin mit, dass die elektronische Anzeigetafel nur die Namen der Bürger anzeige, die elektronisch einen Termin vereinbart hätten. Bei der Buchung eines Online-Termins werde der Nutzer mit folgendem Satz auf die Verfahrensweise beim Aufruf über die Anzeigetafel informiert:
„Tragen Sie zur Bestätigung Ihren Familiennamen (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt) […] ein."
Welchen Namen der Nutzer schlussendlich eingebe, bleibe ihm, dem Bürger, selbst überlassen. So sei es nach Aussage der Stadt auch schon vorgekommen, dass die Bürger ihre Namen selbst gestalteten, sodass auf der Anzeigetafel unter anderem Fantasienamen wie Biene Maja oder Captain Chaos erschienen seien.
Da es somit nicht erforderlich war, den Familiennamen (wie jedoch oben im Text gefordert) anzugeben, riet der TLfDI der Stadt, dies in ihrem Hinweistext aufzunehmen. Zusätzlich sollte der Hinweis aufgenommen werden, wie lange der Name sichtbar ist. Der Text sollte nach Empfehlung des TLfDI wie folgt lauten:
„Tragen Sie zur Bestätigung einen Namen ein (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt. Die Anzeigedauer des von Ihnen eingegeben Namens erstreckt sich bis zum Aufruf des viertnächsten Kunden."
Da zum Ende des Berichtszeitraumes der Sachverhalt noch nicht abgeschlossen war, wird der TLfDI im kommenden Tätigkeitsbericht erneut über diesen kuriosen Fall berichten.

Gemäß dem in § 1 Abs. 2 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) enthaltenen Gebot der Datensparsamkeit kann es in einigen Fällen nicht erforderlich sein, seinen kompletten Familiennamen als Klarnamen bei öffentlichen Stellen anzugeben. Auch ohne die

Nennung des eigenen Namens ist eine Terminvereinbarung bei Behörden möglich, wenn dieser „offenbart“ wird. Biene Maja als Nächste bitte …

5.39 Gemeinderatsmitglieder wollen es wissen: Gehaltshöhe von Geschäftsführern kommunaler Unternehmen. Geht das?

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum mehrere Anfragen von Betroffenen, die Auskunft über die Reichweite des Fragerechts von Gemeinderatsmitgliedern unter Berücksichtigung datenschutzrechtlicher Gesichtspunkte erbaten. Grund hierfür war entweder, dass ein Betroffener als leitender Angestellter eines Eigenbetriebes einer Gemeinde wissen wollte, ob seine Gehaltshöhe und seine Gehaltsstruktur Gegenstand des Fragerechts von Gemeinderatsmitgliedern sein dürfen oder, dass ein Mitglied des Gemeinderats danach fragte, ob er eine besondere Begründung für seine Frage zu der Offenlegung der Gehaltsstruktur von Geschäftsführern kommunaler Betriebe gegenüber der Stadtverwaltung geben müsste. Der TLfDI verwies alle Fragesteller auf das Urteil des Thüringer Oberverwaltungsgerichts (OVG) vom 14. November 2013 (Aktenzeichen 3 KO 900/11). Darin stellten die Richter Folgendes fest:

- Die Frage nach der Vergütung von Geschäftsführen kommunaler Gesellschaften betrifft Angelegenheiten des eigenen Wirkungskreises der Gemeinde, nämlich der Organisation und der Haushaltsführung der von der Gemeinde gegründeten Unternehmen der Daseinsvorsorge.
- Dem Thüringer Kommunalrecht ist ein ungeschriebener Auskunftsanspruch eines Gemeinderatsmitglieds gegenüber dem Bürgermeister, beschränkt durch die Aufgaben der Gemeinde und die Kompetenzen des Gemeinderats, zuzuerkennen.
- Der Auskunftsanspruch folgt nach Ansicht des ThürOVG unmittelbar aus der verfassungsrechtlich vorgegebenen Stellung der Gemeinderatsmitglieder aufgrund einer demokratischen Wahl (Art. 28 Abs. 1 Satz 2 Grundgesetz (GG), Art. 95 der Verfassung des Freistaats Thüringen (ThürVerf)) und des daraus resultierenden freien Mandats, wie ihn einfachgesetzlich § 24 ThürKO normiert.

- Die grundrechtlich geschützten Positionen privater Dritter – insbesondere deren datenschutzrechtliche Belange – werden nach Ansicht des ThürOVG schließlich dadurch hinreichend berücksichtigt, dass die Information an den Gemeinderat in nicht-öffentlicher Sitzung erfolgen soll und somit eine Weitergabe der Daten an unberechtigte Dritte oder die Öffentlichkeit unterbleibt. Denn diese sind von der Teilnahme an der nicht-öffentlichen Sitzung ja gerade ausgeschlossen.
- Die Rechtsauffassung, dass personenbezogene Daten eines Geschäftsführers einer kommunalen Gesellschaft – z. B. solche, die in einem Geschäftsführervertrag enthalten sind – dem Gemeinderat und seinen Mitgliedern nur in nicht-öffentlicher Sitzung bekannt gemacht werden dürfen, entwickelten die Richter des Thüringer OVGs unter Hinweis auf das vom Bundesverfassungsgericht im „Volkszählungs-Urteil“ entwickelte Grundrecht auf informationelle Selbstbestimmung. Dieses Grundrecht hat auch Eingang in die ThürVerf gefunden, nämlich in Art. 6 Abs. 2 ThürVerf. In seinem Urteil hat das ThürOVG den Auskunftsanspruch des Gemeinderatsmitglieds aufgrund Art. 28 Abs. 1 Satz 2 GG und Art. 95 ThürVerf mit dem Grundrecht auf informationelle Selbstbestimmung des Geschäftsführers aus Art. 6 Abs. 2 ThürVerf abgewogen und dabei beide Grundrechte im Rahmen der Problemlösung so zugeordnet, dass jedes Grundrecht Wirklichkeit gewinnt (sog. praktische Konkordanz).

Der TLfDI teilte allen Betroffenen in der Beantwortung ihrer Anfragen mit, dass er diesen vom OVG gefundenen „Kompromiss“ auch datenschutzrechtlich begrüße, da er die personenbezogenen Daten von Geschäftsführern eines kommunalen Betriebes mit der vom Gericht vorgegebenen Vorgehensweise hinreichend geschützt sah.

Des einen Freud’ ist des anderen Leid, sagt der Volksmund. Wenn ein Gemeinderatsmitglied also Auskunft über die Höhe des Gehalts eines Geschäftsführers, einer kommunalen Gesellschaft begehrt, so hat es nach dem Urteil des Thüringer OVGs vom 14. November 2013 (Aktenzeichen: 3 KO 900/11) einen solchen Anspruch auf richtige und vollständige Auskunft. Das gefällt dem betreffenden Geschäftsführer natürlich nicht, weil dadurch sein personenbezogenes Datum, nämlich die Höhe seines Gehalts, übermit-

telt wird. Doch auch dieses Interesse berücksichtigten die OVG-Richter: Denn das Auskunftsersuchen des Gemeinderatsmitglieds darf nur in nicht-öffentlicher Sitzung des Gemeinderats beantwortet werden. Folglich wird das personenbezogene Datum der Gehaltshöhe nur denen übermittelt, die es kennen dürfen – nämlich den Mitgliedern des Gemeinderats im Rahmen ihrer Zuständigkeit nach § 29 Abs. 2 ThürKO.

5.40 Grenzen des Auskunfts- und Akteneinsichtsrechts nach § 13 Thüringer Datenschutzgesetz

Im Berichtszeitraum hatte es der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Fall zu tun, bei dem es um eine Akteneinsicht nach § 13 Thüringer Datenschutzgesetz (ThürDSG) gegenüber dem Landratsamt Altenburger Land ging. Nach § 13 Abs. 1 Satz 3 ThürDSG schließt das Recht auf Auskunft das Recht auf Einsicht in die betreffenden Akten und Dateien ein. Das Landratsamt Altenburger Land verweigerte hier die Einsicht unter Hinweis auf das Vorliegen von Versagungsgründen im Sinne des § 13 Abs. 5 ThürDSG. Gemäß § 13 Abs. 7 ThürDSG muss in einem solchem Fall dem TLfDI Auskunft erteilt werden, soweit nicht das zuständige Landesministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.
Dem anwaltlich vertretenen Beschwerdeführer waren Versagensgründe jedoch nicht ersichtlich, sodass er weiterhin auf die Akteneinsicht nach § 13 ThürDSG bestand. Er bat den TLfDI, das Verfahren nach § 13 Abs. 7 ThürDSG durchzuführen. Dazu fuhr der TLfDI zum Landratsamt Altenburger Land und schaute sich die entsprechende Akte an. Der TLfDI stellte dabei fest, dass die verweigerte Akteneinsicht durch das Altenburger Land aufgrund von Auskunftsverweigerungsgründen i. S. d. § 13 Abs. 5 ThürDSG aus datenschutzrechtlicher Sicht nicht zu beanstanden war. Allerdings darf dann in einem solchen Fall gemäß § 11 Abs. 3 Satz 1 ThürDSG die Mitteilung des TLfDI an den Betroffenen bzw. hier an den bevollmächtigten Rechtsanwalt zu den Erkenntnissen aus der Akteneinsicht des TLfDI keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat. Eine Zustimmung erfolgte in diesem Fall nicht. Somit teilte der TLfDI dem Rechtsanwalt mit, dass

nach dem erfolgten Ortstermin des TLfDI sowie dessen datenschutzrechtlicher Prüfung die Verweigerung der Akteneinsicht auf Grundlage der gesetzlichen Regelung des § 13 Abs. 5 ThürDSG erfolgte und aus datenschutzrechtlicher Sicht nicht zu beanstanden war.
Da in diesem Fall ein verwaltungsrechtliches Klageverfahren in Arbeit war, wies der TLfDI darauf hin, dass hier das zuständige Verwaltungsgericht über die Freigabe der Akten zu entscheiden habe.

Gemäß § 13 Abs. 1 ThürDSG hat die Daten verarbeitende Stelle dem Betroffenen auf Antrag ohne unzumutbare Verzögerung grundsätzlich Auskunft zu erteilen über die zu seiner Person verarbeiteten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind. Dies gilt gemäß § 13 Abs. 1 Satz 2 ThürDSG nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Das Recht auf Auskunft schließt nach § 13 Abs. 1 Satz 3 ThürDSG das Recht auf Einsicht in die betreffenden Akten und Dateien ein. Die Auskunftserteilung und Akteneinsicht unterbleiben jedoch gemäß § 13 Abs. 5 ThürDSG, soweit die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben gefährden würde, die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, die personenbezogenen Daten zur Entscheidung in Gnadensachen oder zur Entscheidung über die Verleihung von staatlichen Orden oder Ehrenzeichen gespeichert sind und schützenswerte, insbesondere datenschutzrechtliche, Interessen Dritter betroffen sind und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

5.41 Kommunale Eigenbetriebe: BDSG oder ThürDSG?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Berichtszeitraum die Rechtsfra-

ge zu entscheiden, ob für den Kommunalservice Jena (KSJ), einem Eigenbetrieb der Stadt Jena, das Bundesdatenschutzgesetz (BDSG) oder das Thüringer Datenschutzgesetz (ThürDSG) anzuwenden ist.
Nach datenschutzrechtlicher Prüfung der Angelegenheit gelangte der TLfDI zu folgender Auffassung:
Für den KSJ ist allein das ThürDSG und nicht das BDSG anwendbar. Dies ergibt sich daraus, dass der KSJ als Eigenbetrieb im Sinne von § 76 Abs. 1 Thüringer Kommunalordnung (ThürKO) keine eigene Rechtspersönlichkeit besitzt (Rücker/Dieter/Schmidt, ThürKO, Kommentar, Band II, § 76, Nr. 1), sondern er unmittelbar von der Gemeinde abhängig ist.
Daran ändert auch die Tatsache nichts, dass gemäß § 76 Abs. 1 Satz 3 ThürKO die Werkleitung eines Eigenbetriebs zur Vertretung nach außen ermächtigt werden kann und im vorliegenden Fall von dieser Regelung in Form einer Bestimmung der gültigen Satzung für den Eigenbetrieb der Stadt Jena „Kommunalservice Jena“ (Satzung) auch Gebrauch gemacht worden ist. Dies ergibt sich zum einen daraus, dass im Text der Satzung noch einmal feststellt wird, dass der Eigenbetrieb KSJ keine eigene Rechtspersönlichkeit besitzt. Zum anderen wird die organisatorische, verwaltungsmäßige und finanzwirtschaftliche Eigenständigkeit des KSJ von der Stadt Jena durch die Satzung begrenzt. Danach führt die Werkleitung die laufenden Geschäfte des Eigenbetriebes. Bei der Beantwortung der Frage, wie der Begriff der „laufenden Geschäfte der Werkleitung“ gemäß § 76 Abs. 1 Satz 2 ThürKO konkret zu definieren ist, ist eine analoge Anwendung von § 29 Abs. 2 Nr. 1 ThürKO zulässig (so Rücker/Dieter/Schmidt, ThürKO, Kommentar, Band II, § 76, Nr. 3.1.1). Danach sind laufende Angelegenheiten des eigenen Wirkungskreises der Gemeinde solche, die für die Gemeinde keine grundsätzliche Bedeutung haben und keine erheblichen Verpflichtungen erwarten lassen. Demgegenüber hat die Einhaltung datenschutzrechtlicher Regelungen und die Kontrolle durch einen Datenschutzbeauftragten in einem Eigenbetrieb einer öffentlichen Stelle eine hohe und damit grundsätzliche Bedeutung, was nicht zuletzt durch den Regelungsgehalt des § 10a ThürDSG – der Bestellung eines Datenschutzbeauftragten – zum Ausdruck kommt. Auch entstehen erhebliche finanzielle wie auch datenschutzrechtliche Verpflichtungen, wenn ein Eigenbetrieb einer Kommune als öffentliche Stelle einen (eigenen) Datenschutzbeauftragten bestellt.

Die o. g. Argumente führten zu dem Ergebnis, dass für den KSJ als Eigenbetrieb im Sinne von § 76 ThürKO ausschließlich das ThürDSG anzuwenden ist. Daraus folgte weiterhin, dass gemäß § 10a ThürDSG ein Mitarbeiter der Stadt Jena bzw. des KSJ als Datenschutzbeauftragter zu bestellen ist.
Die Stadtverwaltung Jena ist dieser Forderung des TLfDI zunächst nicht gefolgt, einen Mitarbeiter bzw. eine Mitarbeiterin der Stadt Jena bzw. des KSJ als Datenschutzbeauftragten zu bestellen. Vielmehr sollte weiterhin das Auftragsverhältnis zwischen dem KSJ und dessen externem Datenschutzbeauftragen beibehalten werden.
Im Ergebnis stellte der TLfDI fest, dass ein für den KSJ zuständiger bzw. mitzuständiger Datenschutzbeauftragter gemäß § 10a ThürDSG entgegen der Forderung des TLfDI nicht bestellt wurde und beanstandete daher gemäß § 39 Abs. 1 Satz 1 ThürDSG die rechtswidrige Nichtbestellung eines internen Datenschutzbeauftragten für den Eigenbetrieb der Stadt Jena KSJ. Zugleich forderte der TLfDI die Stadt Jena auf, gemäß § 10a ThürDSG einen Mitarbeiter der Stadt Jena bzw. des KSJ als Datenschutzbeauftragten des KSJ zu bestellen und dies durch die Vorlage der Bestellungsurkunde nachzuweisen.
Daraufhin teilte der Oberbürgermeister der Stadt Jena dem TLfDI mit, dass nunmehr die Datenschutzbeauftragte der Stadtverwaltung Jena gemäß § 10a ThürDSG auch für alle Eigenbetriebe der Stadt Jena, einschließlich des KSJ, zuständig und der bisherige externe Datenschutzbeauftragte des KSJ von seiner Funktion entbunden worden sei. Damit war die Stadt Jena den Forderungen des TLfDI vollumfänglich nachgekommen.

Da kommunale Eigenbetriebe im Sinne von § 76 ThürKO keine eigene Rechtspersönlichkeit haben, ist für sie ausschließlich das ThürDSG anzuwenden, verbunden mit der Folge, dass auch ein Mitarbeiter des Eigenbetriebes bzw. der Gemeinde als Datenschutzbeauftragter auf der Grundlage von § 10a ThürDSG zu bestellen ist.

5.42 Global Positioning System (GPS) für Kommunalbedienstete

Eine Stadtverwaltung wollte GPS (Global Positioning System)-Daten zum Zweck der Tourenplanung und Organisation ihrer Fahrzeugflotte verarbeiten und nutzen und bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung im Hinblick auf den Beschäftigtendatenschutz.

Der TLfDI teilte mit, dass zunächst zu prüfen ist, welche konkreten Daten für den festgelegten Zweck erforderlich sind (§ 19 Abs. 1 Thüringer Datenschutzgesetz – ThürDSG). Dabei ist zu berücksichtigen, dass die erfassten Daten, soweit sie auf den jeweiligen Fahrer bezogen werden können, personenbezogene Daten im Sinne des § 3 Abs. 1 ThürDSG darstellen. GPS-Systeme ermöglichen die Erfassung einer Vielzahl von Einzeldaten. Für die Tourenplanung und die Organisation der Fahrzeugflotte war aus Sicht des TLfDI lediglich eine Positionserfassung der Fahrzeuge erforderlich. Die auf diese Art und Weise erhobenen Daten dürfen auch nur so lange gespeichert werden, wie sie zur Aufgabenerfüllung erforderlich sind. Für die dargelegten Zwecke war eine Speicherung für einen längeren Zeitraum nicht erforderlich, vielmehr war ein aktueller Zugriff ausreichend. Eine Speicherung über den Tag hinaus wäre nicht zu rechtfertigen gewesen.
Im Zusammenhang mit der Erbringung der Leistungen für den Winterdienst können beim Einsatz von GPS über die Positionsdaten hinaus weitere Vorgänge erfasst werden. Hierzu zählen beispielsweise die Nutzung des Schneepflugs und die Menge des ausgestreuten Salzes. Für die Beantwortung von Beschwerden von Anwohnern oder Anfragen der Polizei im Zusammenhang mit Verkehrsunfällen können zum Nachweis der Leistungserbringung die Daten für einen festzulegenden kurzen Zeitraum gespeichert werden.
Da aber immer ein Bezug zu den Fahrern hergestellt werden kann, ist im Hinblick auf die betroffenen Beschäftigten zu beachten, dass eine Leistungs- und Verhaltenskontrolle mittels Auswertung der Positionsdaten nach § 33 Abs. 4 ThürDSG nicht zulässig ist.
In der erforderlichen Dienstvereinbarung oder Dienstanweisung müsste aus Gründen der Transparenz für die betroffenen Fahrer und Mitarbeiter zwingend festgelegt werden, welche konkreten Daten erfasst werden und für welchen Zeitraum diese von wem unter welchen Voraussetzungen und zu welchem Zweck ausgewertet werden können.

Soll GPS-Technik für konkrete Zwecke verarbeitet und genutzt werden, muss in der entsprechenden Dienstvereinbarung genau festgelegt werden, welche Daten für welchen Zweck wie lange gespeichert werden dürfen und wer unter welchen Voraussetzungen und zu welchem Zweck die Daten nutzen darf. Eine Leistungs- und Verhaltenskontrolle der Mitarbeiter ist unzulässig und daher auszuschließen.

5.43 Weitergabe einer Telefonnummer zur Verfolgung einer Ordnungswidrigkeit

Die Polizeiinspektion Eichsfeld übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) einen dienstlichen Vermerk zu einer Anzeige über die Herausgabe einer privaten Telefonnummer durch die Wohnungsverwaltung der Verwaltungsgemeinschaft Niederorschel an das zuständige Ordnungsamt.
Hintergrund der Angelegenheit war ein seit längerem dauernder Streit über die Nutzung eines Anwohnerparkplatzes, den der Beschwerdeführer von der Wohnungsverwaltung gemietet hatte. Anlass der polizeilichen Anzeige des Beschwerdeführers war ein Anruf des Ordnungsamtes beim Beschwerdeführer zu o. g. Angelegenheit, wobei das Ordnungsamt mitteilte, die Telefonnummer des Beschwerdeführers von der Wohnungsverwaltung erfahren zu haben.
Nach Auffassung des Beschwerdeführers sei die Übermittlung seiner Telefonnummer nicht zulässig, da er in deren Herausgabe nicht eingewilligt habe und sie auch nicht in öffentlichen Verzeichnissen eingesehen bzw. recherchiert werden könne.
Der TLfDI forderte die Wohnungsverwaltung zur Stellungnahme in der Angelegenheit auf. Die Wohnungsverwaltung teilte dem TLfDI mit, dass die Telefonnummer des Beschwerdeführers auf Anfrage des Ordnungsamts zum Zwecke der Verfolgung einer Ordnungswidrigkeit wegen nicht vorschriftsgemäßer Nutzung eines Parkplatzes übermittelt worden sei, um mit dem Beschwerdeführer Kontakt aufnehmen zu können.
Nach Auffassung des TLfDI handelt es sich hierbei um eine Datenübermittlung innerhalb des öffentlichen Bereichs, deren Zulässigkeit nach § 21 i. V. m. § 20 Thüringer Datenschutzgesetz (ThürDSG) zu beurteilen ist. Gemäß § 21 Abs. 1 ThürDSG ist eine solche Übermittlung zulässig, wenn sie 1. zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Dritten erforderlich ist – dies konnte im vorliegenden Fall für das Ordnungsamt bejaht werden – und 2. die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Nach § 20 Abs. 2 Nr. 7 ThürDSG ist das Speichern, Verändern oder Nutzen für andere Zwecke unter anderem zulässig, wenn es zur Verfolgung von Ordnungswidrigkeiten erforderlich ist. Im vorliegenden Fall forderte das Ordnungsamt gerade die Adresse

des Beschwerdeführers von der Wohnungsverwaltung an, um eine Ordnungswidrigkeit zu verfolgen. Der TLfDI sah auch keine andere Möglichkeit, wie das Ordnungsamt ansonsten mit dem Beschwerdeführer hätte in Kontakt treten können. Der TLfDI ging daher im Ergebnis von einer zulässigen Datenübermittlung für andere Zwecke aus.

Unter den engen Zulässigkeitsvoraussetzungen des § 20 Abs. 2 Nr. 1 bis 9 ThürDSG kann das Speichern, Verändern – das auch eine Datenübermittlung beinhaltet – oder Nutzen personenbezogener Daten für andere Zwecke (Zweckänderung) zulässig sein.

5.44 Fotosafari im Schlafzimmer oder eine mitteilsame Waffenbehörde

Ein Betroffener setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum über eine mutmaßlich unzulässige Weitergabe personenbezogener Daten durch einen Mitarbeiter der Waffenbehörde eines Landratsamtes in Kenntnis.
Zur „Vorgeschichte“ der Angelegenheit teilte der Betroffene mit, dass er Jäger und Inhaber eines Jagdscheins sowie einer Waffenbesitzkarte sei und daher legal Schusswaffen und Munition besitzen dürfe. Infolge einer anonymen Strafanzeige wegen eines Verstoßes gegen das Waffengesetz sei ein Strafverfahren gegen ihn eröffnet worden. Im Rahmen dieses Strafverfahrens hätten die Waffenbehörde eines Landkreises und die ermittelnden Polizeibeamten eine Hausdurchsuchung bei ihm als Betroffenem durchgeführt und dabei Fotos der Wohnung einschließlich seines Schlafzimmers gefertigt und Waffen und Munition beschlagnahmt. Nachfolgend habe das zuständige Amtsgericht diese Hausdurchsuchung für rechtswidrig erklärt, die Beschlagnahme der aufgefundenen Schusswaffen und Munition aufgehoben und das Strafverfahren gegen den Betroffenen eingestellt.
Später habe ein Mitarbeiter der Waffenbehörde dem Leiter des Hegerings (einer Organisationeinheit der Jägerschaft), dem auch der Betroffene angehört, Einzelheiten zur Hausdurchsuchung mitgeteilt und angeboten, die dabei gefertigten Fotos der Wohnung des Betroffenen zu zeigen. Da der Zustand der Wohnung schlampig gewesen sei, könne der Hegering ggf. Disziplinarmaßnahmen gegen den

Betroffenen einleiten. Zudem sei dem Leiter des Hegerings in der Waffenbehörde die Verwaltungsakte des Betroffenen mit den im Rahmen der Hausdurchsuchung gefertigten Fotos vorgelegt worden.

Der TLfDI teilte dem Betroffenen mit, dass es sich bei dem dargelegten Sachverhalt um eine unbefugte bzw. zweckwidrige Übermittlung bzw. Weitergabe von personenbezogenen Daten, die nicht offenkundig seien, handeln könnte. In diesem Zusammenhang kämen folgende Verstöße infrage:

1. Eine Ordnungswidrigkeit im Sinne von § 43 Abs. 1 oder 2 Thüringer Datenschutzgesetz (ThürDSG) oder
2. eine Straftat im Sinne von § 43 Abs. 3 ThürDSG unter der zusätzlichen Voraussetzung, dass die o. g. Handlung mit der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, getätigt wurde.

Der TLfDI kontrolliert u. a. die Einhaltung datenschutzrechtlicher Bestimmungen bei öffentlichen Stellen Thüringens und beanstandet die dort festgestellten datenschutzrechtlichen Verstöße. Der TLfDI ist hingegen nicht die zuständige Behörde zur Verfolgung und Ahndung von datenschutzrechtlichen Ordnungswidrigkeiten im öffentlichen Bereich. Zuständig ist nach § 36 Abs. 2 des Gesetzes über Ordnungswidrigkeiten (OWiG) in Verbindung mit § 8 der Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Innenministeriums diejenige Behörde, der der Vollzug derjenigen Rechtsvorschrift obliegt, gegen die sich der Verstoß richtet.
Sofern eine Straftat im Sinne von § 43 Abs. 3 ThürDSG vorliegt, kann eine solche Tat auf Antrag verfolgt werden; antragsberechtigt sind der Betroffene und der TLfDI. Insofern besteht für den TLfDI die Möglichkeit, einen entsprechenden Antrag bei der zuständigen Staatsanwaltschaft zu stellen.
Der Betroffene bat den TLfDI, die Angelegenheit zur strafrechtlichen Verfolgung an die zuständige Staatsanwaltschaft abzugeben und Strafantrag gegen die jeweils handelnden Behördenmitarbeiter zu stellen. Dies sah auch der TLfDI aus folgenden Gründen als sachdienlich an:
Es bestand der Anfangsverdacht, dass die rechtswidrige Bekanntgabe des Akteninhalts an eine verfahrensfremde Privatperson, insbesonde-

re die Gewährung der Einsichtnahme in Fotos der Wohnung mit dem Wohn- und Schlafzimmer (die einen besonders geschützten Persönlichkeitsbereich zeigten), einzig zu dem Zweck erfolgte, den Betroffenen in der Öffentlichkeit herabzuwürdigen und verächtlich zu machen. Deshalb war nach Auffassung des TLfDI insoweit auch der Straftatbestand des § 43 Abs. 3 ThürDSG erfüllt, denn die Handlung des Mitarbeiters der Waffenbehörde erfolgte, um den Betroffenen zu schädigen.
Nachfolgend stellte der TLfDI einen Strafantrag gegen Unbekannt gemäß § 43 Abs. 3 Satz 2 und Satz 3 ThürDSG wegen Verstoßes gegen das Thüringer Datenschutzgesetz. Daraufhin bestätigte die zuständige Staatanwaltschaft gegenüber dem TLfDI den Eingang seines Strafantrages. Das strafrechtliche Ermittlungsverfahren wurde bislang noch nicht abgeschlossen. Der TLfDI wird daher nach Abschluss der strafrechtlichen Ermittlungen diesen Fall im nächsten Tätigkeitsbericht wieder aufgreifen.

In Fällen eines datenschutzrechtlichen Verstoßes gemäß § 43 Abs. 3 ThürDSG, in denen der Täter gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, ist der TLfDI befugt, zu einem scharfen Schwert zu greifen und einen Strafantrag bei der zuständigen Staatsanwaltschaft zu stellen. Das Strafmaß für eine solche Tat ist Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

5.45 Individuelle Hilfeplanung: Datenverarbeitung nur bei datenschutzgerechter Einwilligungserklärung

Um Eingliederungshilfe als Betroffener nach den §§ 53, 54 Sozialgesetzbuch – Zwölftes Buch (SGB XII) in Anspruch nehmen zu können, wird von der zuständigen Sozialbehörde mit einem individuellen Hilfeplan der persönliche Unterstützungsbedarf ermittelt. Die Erfassung der hierfür erforderlichen personenbezogenen Daten der Hilfsbedürftigen erfolgte seitens des zuständigen Sozialamts einer kreisfreien Stadt in Thüringen formularmäßig. Aufgrund eines Hinweises auf die umfangreiche Erhebung von Gesundheitsdaten und Diagnosen der Betroffenen und im Hinblick auf die Frage, wie der Datenschutz bei Beteiligung einer Vielzahl von Personen an der Erstellung dieses Planes gewährleistet sei, unterzog der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit

(TLfDI) das im Internet verfügbare Formular einer eingehenden datenschutzrechtlichen Prüfung.
Zur Erhebung waren auf diesem Formblatt neben Angaben zu den „im Moment“ vorhandenen Hilfen und Gegebenheiten eine Vielzahl von Wünschen und Vorstellungen des Betroffenen zur zukünftig angestrebten Wohn- und Lebensform einzutragen, die vom Sozialamt aus fachlicher Sicht ergänzt werden konnten. Mit der Unterschrift des Betroffenen und ggf. seines Betreuers am Ende des Formulars sollten die Information über die Datenverarbeitung im Merkblatt bestätigt und gleichzeitig auch alle beteiligten Mitarbeiter der betreffenden Stadtverwaltung von der Schweigepflicht entbunden werden.
Diese Form des Antrags entsprach nicht den gesetzlichen Anforderungen an den Datenschutz. Nach dem Wortlaut von § 67b SGB X ist der Betroffene, sofern die Einwilligung bei ihm eingeholt wird, auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform. Soll die Einwilligung, wie hier, zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie im äußeren Erscheinungsbild der Erklärung hervorzuheben. Für die Wirksamkeit der datenschutzrechtlichen Einwilligungserklärung ist es erforderlich, dass die Sozialdaten genau festgelegt werden, auf die sich die Verarbeitung oder Nutzung bezieht. Weiterhin müssen die Stellen festgelegt werden, die zur Verarbeitung oder Nutzung berechtigt sein sollen. Auch der Verarbeitungs- und Nutzungszweck ist hinreichend festzulegen. Von der Erteilung der Einwilligung nach § 67b Abs. 1 SGB X ist die Schweigepflichtentbindung zu unterscheiden, die eine Strafbarkeit der beteiligten Personen nach § 203 Strafgesetzbuch verhindert, sofern es sich dabei um Berufsgeheimnisträger handelt. Diese Einwilligung bedarf grundsätzlich keiner bestimmten Form. Die Schweigepflichtentbindung kann zwar grundsätzlich mit der datenschutzrechtlichen Einwilligungserklärung verbunden werden, stellt aber selbst keine Befugnis zur Datenverarbeitung dar.
Der TLfDI forderte das Sozialamt auf, die datenschutzrechtliche Einwilligungserklärung nach einem Text abgeben zu lassen, der den Inhalt des Merkblatts zumindest im Wesentlichen wiedergibt. Daraufhin wurden das Merkblatt und das veröffentlichte Formular überarbeitet. Mit der am Ende des Formblatts vorgesehenen Unter-

schrift erteilt der betroffene Antragsteller bzw. sein Bevollmächtigter oder Betreuer die Einwilligung, die zum Zweck der Durchführung des Hilfeplangesprächs erhobenen Daten dem sozialpsychiatrischen Dienst und ggf. weiteren Teilnehmern zu übermitteln, wenn er damit einverstanden ist. Dabei kann der Betroffene den Personenkreis durch Streichungen reduzieren. Damit wurde dem datenschutzrechtlichen Anliegen des TLfDI Rechnung getragen.

Ist zur Erhebung und Verarbeitung von Sozialdaten die Einwilligung des Betroffenen vorgesehen, ist er auf den konkreten Zweck der Datenverarbeitung hinzuweisen. Es muss möglich sein, die Einwilligung auf bestimmte Arten von Daten oder bestimmte Arten der Verarbeitung zu beschränken. Bei der Übermittlung muss der empfangsberechtigte Personenkreis durch den Betroffenen bestimmbar sein. Die Einwilligung muss auf seiner freien Entscheidung beruhen.

5.46 Beschlüsse von Stadtratssitzungen können grundsätzlich im Netz veröffentlicht werden!

Ein Beschwerdeführer setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber in Kenntnis, dass der Inhalt des öffentlichen Teils einer Sitzung des Stadtrates Eisenach samt einer Vorschlagsliste für Schöffen einschließlich der Namen und Anschriften der Betroffenen ins Internet gestellt worden sei.
Der TLfDI bat daraufhin die Stadtverwaltung Eisenach, mitzuteilen, auf welcher Rechtsgrundlage diese Übermittlung personenbezogener Daten beruhte und zu welchem Zwecke sie erfolgte.
Nachfolgend teilte die Stadtverwaltung Eisenach dem TLfDI mit, dass sie im Jahr 2009 ein Ratsinformationssystem eingeführt habe, worüber die Beschlüsse des Stadtrates interessierten Bürgern auf der städtischen Internetseite zur Verfügung gestellt würden. Dabei achte die Stadt Eisenach darauf, dass keine personenbezogenen Daten im Internet veröffentlicht würden.
Die Stadtratsbeschlüsse, die vor 2009 gefasst worden seien, seien ebenfalls im Internet zu finden gewesen. Dabei sei versehentlich auch der Beschluss zur Schöffenwahl mit Namen und Anschriften der vorgeschlagenen Schöffen unter den öffentlichen Bekanntmachungen der Beschlüsse eingestellt worden. Unmittelbar nach Eingang des Schreibens des TLfDI habe die Stadtverwaltung die Be-

schlüsse aus den Jahren vor 2009 von der städtischen Internetseite genommen.
Hiervon hat sich der TLfDI überzeugt und deshalb die Beschwerde als erledigt angesehen.

Unter der Voraussetzung, dass keine personenbezogenen Daten veröffentlicht werden, spricht aus datenschutzrechtlicher Sicht nichts dagegen, den Inhalt öffentlicher Beschlüsse kommunaler Gremien auf die Webseite der Kommune zu stellen. Dies erfordert jedoch neben einem zusätzlichen Arbeitsaufwand datenschutzrechtliche Kenntnisse und redaktionelles Geschick.

5.47 Keine Telefonauskünfte an Unbekannte!

Ein Betroffener beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass das Wahlbüro des Landratsamtes Nordhausen Daten zu seiner Person an einen Dritten übermittelt hätte.
Zunächst habe der Betroffene per E-Mail das Wahlbüro beim Landratsamt Nordhausen zum Zwecke seiner Kandidatur für die Bundestagswahl angeschrieben. Daraufhin habe ein Mitarbeiter des Wahlbüros mit einem Dritten telefonisch über die persönlichen Daten des Betroffenen aus dessen E-Mail gesprochen und gebeten, dem Betroffenen auszurichten, dass er das Wahlbüro anrufen möchte. Der Betroffene gab an, dass die Telefonnummer des Dritten nicht von ihm preisgegeben worden sei und daher aus einer anderen Quelle stammen müsste.
Der TLfDI forderte das Landratsamt auf, zu den Beschwerdepunkten Stellung zu nehmen und mitzuteilen, zu welchen Zwecken eine dritte Person in einer Angelegenheit des Betroffenen telefonisch kontaktiert und dieser Person personenbezogene Daten des Betroffenen mitgeteilt wurden sowie auf welchen Rechtsgrundlagen dieses Handeln beruhte.
Das Landratsamt Nordhausen setzte den TLfDI daraufhin darüber in Kenntnis, dass das Wahlbüro offene Fragen zur E-Mail des Betroffenen, mit der er sich als Kandidat für die Bundestagswahl beworben hatte, schnellstmöglich klären wollte. Hierzu sei anhand der Anschrift aus der o. g. E-Mail per Internet ein Telefonanschluss mit dem Nachnamen des Betroffenen recherchiert worden. Daraufhin habe das Wahlbüro unter dieser Telefonnummer eine Frau, bei der es

sich nach deren eigenen Angaben um die Großmutter des Betroffenen gehandelt habe, angerufen. Hierbei seien Fragen zu Angaben des Betroffenen, die dieser im Zusammenhang mit seiner Wahlkandidatur gemacht habe, erörtert worden. Abschließend habe das Wahlbüro gebeten, dem Betroffenen auszurichten, er möge das Wahlbüro anrufen. Nachfolgend habe das Wahlbüro eine E-Mail an den Betroffenen mit der Bitte um Rückruf gesandt.
Das Landratsamt teilte die Auffassung des TLfDI, dass die telefonische Mitteilung von personenbezogenen Daten gegenüber Dritten mangels Rechtsgrundlage einen datenschutzrechtlichen Verstoß darstellte.
Aufgrund der verbindlichen Zusage des Landratsamtes Nordhausen, künftig dafür Sorge zu tragen, dass derartige Fehler nicht wiederholt werden, sah der TLfDI die Angelegenheit als erledigt an. Der TLfDI wies das Landratsamt jedoch abschließend darauf hin, dass die Übermittlung personenbezogener Daten nicht über das unsichere Übertragungsmedium einer unverschlüsselten E-Mail erfolgen dürfe.

Auch wenn eine öffentliche Stelle im Sinne eines Betroffenen offene Fragen am Telefon klären will, gilt für sie die Regelung des § 4 Abs. 1 ThürDSG, die eine Verarbeitung und Nutzung personenbezogener Daten nur dann für zulässig erklärt, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Mitarbeiter des Wahlbüros hätten im konkreten Fall also von dem Betroffenen erst einmal dessen Einwilligung einholen müssen, ob sie mit der dritten Person am Telefon über die personenbezogenen Daten des Betroffenen reden durften bzw. hätten die Daten nach § 19 Abs. 2 S. 1 ThürDSG beim Betroffenen selbst erhoben werden müssen.

5.48 Keine Umfrage ohne Datenschutzhinweis

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Bedarfsermittlung zur Nutzung von Digital Subscriber Line- (DSL) bzw. Breitbandversorgung zum Zweck der Internetversorgung in der Stadt Bad Frankenhausen in Kenntnis und bat um Prüfung des verwendeten Fragebogens.
Der TLfDI stellte zunächst fest, dass der verwendete Fragebogen, der neben dem Namen und der Anschrift des Inhabers des Internet-

anschlusses auch Angaben zu dessen derzeitigem und zum gewünschten Internetanschluss wie Bandbreite, Flatrate und Nutzungsart (Surfen, E-Mail, Online-Banking, Filme schauen) beinhaltete, personenbezogene Daten erfasste und dabei keine Hinweise zum Datenschutz enthielt. Der TLfDI bat deshalb die Stadtverwaltung Bad Frankenhausen um Beachtung folgender Hinweise:

Gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Im Falle der Einwilligung ist die Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit sie zur Erfüllung anerkannter Zwecke erforderlich ist. Im vorliegenden Fall war für den TLfDI zunächst fragwürdig, ob die Erhebung der personenbezogenen Daten für den Zweck einer DSL-/Breitbandumfrage überhaupt erforderlich sei. Aber selbst, wenn der TLfDI diese Frage bejahte, enthielt der besagte Fragebogen keine konkrete Einwilligung des Befragten, dass die Stadtverwaltung Bad Frankenhausen diese erhobenen personenbezogenen Daten verarbeiten und nutzen durfte. Auf eine solche Einwilligung kam es im konkreten Sachverhalt aber gerade an.

Werden personenbezogene Daten beim Betroffenen erhoben, so sind nach § 19 Abs. 3 ThürDSG die Identität der Daten verarbeitenden Stelle, der Erhebungszweck sowie im Fall vorgesehener Übermittlung der Empfänger der Daten dem Betroffenen gegenüber anzugeben. Auf die Freiwilligkeit seiner Angaben ist der Betroffene hinzuweisen.

All diese Hinweise fehlten im konkreten Fragebogen der Stadtverwaltung Bad Frankenhausen. Der TLfDI forderte die Stadtverwaltung deshalb auf, die Fragebögen um einen entsprechenden Hinweis nach § 19 Abs. 3 ThürDSG zu ergänzen.

Die Stadtverwaltung setzte den TLfDI darüber in Kenntnis, dass der verwendete Fragebogen auf einem Muster beruhte, den das Breitbandkompetenzzentrum Thüringen der Landesentwicklungsgesellschaft Thüringen mbH auf seiner Internetseite zum Abruf bereithielte. Im Zuge weiterer Recherchen teilte das Breitbandkompetenzzentrum Thüringen mit, dass dessen Musterfragebogen vor einiger Zeit überarbeitet worden sei und das „Formular (-Muster) zur Bedarfsermittlung“ auf http://www.thüringen-

online.de/ unter den Menüpunkten „Service“, „Download“, „Anträge und Formulare“ zum Download bereit stünde. Der TLfDI überzeugte sich von der Datenschutzkonformität des überarbeiteten Musterfragebogens.
Da dem von der Stadtverwaltung Bad Frankenhausen verwendeten Fragebogen möglicherweise eine ältere Version ohne die erforderlichen Hinweise zum Datenschutz zugrunde lag, forderte der TLfDI die Stadt Bad Frankenhausen auf, den Fragebogen entsprechend seiner o. g. Hinweise zu überarbeiten bzw. auf den aktuellen Musterfragebogen des Breitbandkompetenzzentrums Thüringen zurückzugreifen und die bisher verwendeten Fragebögen durch die überarbeitete Fassung zu ersetzen.
Nachfolgend teilte die Stadtverwaltung Bad Frankenhausen dem TLfDI mit, dass sie die Bedarfsermittlung vorzeitig beendet und alle ausgelegten Fragebögen eingesammelt sowie den Fragebogen von der Internetseite der Stadt Bad Frankenhausen entfernt habe.

„Wer nicht fragt bleibt dumm“ – lautet schon die Feststellung einer bekannten deutschen Kinderserie. Zu beachten ist aber für eine Kommune, dass sie bei einer Verwendung von Fragebögen, die personenbezogene Daten erheben sollen, auch den Datenschutz hinreichend beachtet. Für den Fall, dass eine geeignete Rechtsgrundlage zur Durchführung einer Erhebung/Umfrage fehlt, ist die Datenerhebung auf der Grundlage einer Einwilligung des Betroffenen nur unter den Voraussetzungen des § 19 Abs. 3 Satz 1 ThürDSG durchzuführen. Das heißt: Der Betroffene, der seine Einwilligung erteilen soll, ist auf den Zweck und den Umfang der Datenverarbeitung und -nutzung, auf die voraussichtliche Dauer der Speicherung seiner Daten und auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

5.49 Offene Briefe vom Finanzamt

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum mit, dass ein Schreiben des Finanzamtes Pößneck unverschlossen an ihn zugestellt worden sei.
Das Finanzamt Pößneck bestätigte gegenüber dem TLfDI diesen Sachverhalt und bestätigte, dass die Klebevorrichtung bzw. -technik

in der Poststelle des Amtes versagt habe. Zugleich sicherte das Finanzamt zu, alles zu unternehmen, damit sich ein solches Vorkommnis nicht wiederhole und entschuldigte sich gegenüber dem Beschwerdeführer. Nach Prüfung der Angelegenheit sah der TLfDI deshalb von einer datenschutzrechtlichen Beanstandung des Vorkommnisses nach § 39 Thüringer Datenschutzgesetz (ThürDSG) ab.
Wenige Wochen später erreichte den TLfDI allerdings ein weiteres Schreiben desselben Beschwerdeführers, der über ein zweites unverschlossenes Schreiben des Finanzamtes Pößneck informierte. So sei dem Beschwerdeführer eine Lohnsteuerbescheinigung, aus der das Einkommen als „Nichtselbstständiger“ erkennbar gewesen sei, ebenfalls unverschlossen übersandt worden.
Da es aus datenschutzrechtlicher Sicht somit ein grundlegendes Problem bei der Postzustellung durch das Finanzamt zu geben schien, bat der TLfDI das Finanzamt um erneute und eingehende Stellungnahme zum Sachverhalt. Vorsorglich wies der TLfDI das Finanzamt auf seine Unterstützungs- und Auskunftspflicht gemäß § 38 ThürDSG hin und teilte mit, dass, falls der Sachverhalt nicht vollends aufgeklärt werden könne und die datenschutzrechtlichen Verstöße im Finanzamt weiterhin andauerten, sich der TLfDI es vorbehalte, das Finanzamt einer datenschutzrechtlichen Kontrolle gemäß § 37 ThürDSG zu unterziehen.
Daraufhin teilte das Finanzamt dem TLfDI mit, dass durch Lagerdauer, Lagerort oder den Transport der Briefsendungen die selbstklebende Eigenschaft der selbstklebenden Briefumschläge nachgelassen haben und somit ein technisches Versagen nicht ausgeschlossen werden könnte. Jedoch habe das Finanzamt die Angelegenheit nicht restlos aufklären können, unter anderem weil der Beschwerdeführer nicht bereit gewesen sei, die mutmaßlich mangelhaften Briefumschläge dem Finanzamt vorzulegen. Jedoch habe das Finanzamt seine Bediensteten angewiesen, die betroffenen Briefumschläge nicht mehr zu verwenden und die Kuverts mittels Klebestreifen bzw. Klebestift selbst und sicher zu verschließen. Auch sagte das Finanzamt zu, künftig bei der Beschaffung sorgfältiger auf die Qualität der Kuverts zu achten und die Ausgangspost regelmäßig zu kontrollieren.
Da die vom Finanzamt getroffenen Maßnahmen eine datenschutzkonforme Zustellung seiner Post erwarten ließen und dem TLfDI ferner keine weiteren unverschlossenen Briefe des Finanzamts be-

kannt wurden, waren keine weiteren Kontrollmaßnahmen vom TLfDI zu veranlassen.

Gerade im „Massengeschäft“ der Finanzverwaltung kann eine strikte Qualitätskontrolle, z. B. in Form von Stichproben, eine wichtige technisch-organisatorische Maßnahme nach § 9 ThürDSG sein, um Verstößen gegen datenschutzrechtliche Vorschriften vorzubeugen.

5.50 Grabstelleninhaber wider Willen

Wie der Presse zu entnehmen war, hatte das Garten- und Friedhofsamt Erfurt einen Bürger aus Neu-Ulm als Nutzungsberechtigten einer Grabstelle angeschrieben. Später stellte sich jedoch heraus, dass der Betroffene kein Grab in Erfurt nutzte.
Daher bat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Stadtverwaltung Erfurt, zu der Angelegenheit Stellung zu nehmen und insbesondere konkret mitzuteilen, wie es zu dieser Verwechslung bzw. Fehlnutzung personenbezogener Daten kommen konnte und auf welche Weise, ggf. durch Änderung der Arbeitsabläufe, dies künftig in ähnlichen Fällen ausgeschlossen werden könnte.
Die Stadtverwaltung Erfurt setzte den TLfDI sodann darüber in Kenntnis, dass in diesem Falle die Altdaten nicht korrekt abgeglichen worden seien. Zwar sei eine Person gleichen Namens festgestellt worden, die ehemals in Erfurt gewohnt habe und danach nach Neu-Ulm verzogen sei. Aber deren Erfurter „Altadresse“ habe nicht der im Friedhofs-Informations-Management vorgehaltenen Adresse entsprochen; jedoch sei dem zuständigen Mitarbeiter des Friedhofamtes diese Nichtübereinstimmung nicht aufgefallen.
Die Stadtverwaltung sagte zu, die betreffenden Mitarbeiter nochmals ausdrücklich darauf hinzuweisen, bei der Prüfung darauf zu achten, dass die der Stadtverwaltung vorliegenden Altdaten vollständig mit den Einwohnermeldedaten übereinstimmen müssten, ehe eine vermeintlich neue Adresse genutzt werde. Zusätzlich prüfe zukünftig ein weiterer Mitarbeiter die Ergebnisse der Recherche.
Des Weiteren würde bei Neuerfassungen von Adressen im Friedhofs-Informations-Management seit geraumer Zeit das Geburtsdatum miterfasst, um künftige Nachforschungen sicherer zu machen. Da die Mitarbeiter entsprechend sensibilisiert worden seien, könne eine derartige Verwechslung künftig ausgeschlossen werden. Auch

habe die Stadtverwaltung zwischenzeitlich Kontakt mit dem Betroffenen aufgenommen. Der TLfDI sah die Angelegenheit damit im Ergebnis als erledigt an.

Recherchevorgänge sind mittels geeigneter technisch-organisatorischer Maßnahmen, auch im Sinne von § 9 ThürDSG so zu organisieren, dass eine Verwechslung von Personen und ihren personenbezogenen Daten ausgeschlossen werden kann. Dies gilt auch bei personenbezogenen Daten von Nutzungsberechtigten einer Friedhofsgrabstelle.

5.51 Zulässigkeit des Verfahrens E-POSTBUSINESS-BOX

Ein Landratsamt bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die datenschutzrechtliche Beurteilung des Einsatzes des E-POSTBUSINESS-BOX-Verfahrens und legte den Entwurf eines Vertrages zur Datenverarbeitung im Auftrag zwischen dem Landratsamt (Auftraggeber) und einem Postdienstleister (Auftragnehmer) vor. Konkret war vorgesehen, dass die Poststelle des Landratsamtes mittels des Verfahrens E-POSTBUSINESS-BOX Massendrucksachen ohne Unterschriftserfordernis, wie z. B. für Schreiben zu Hortgebühren, bearbeitet.
Bei dem Verfahren wird die Ausgangspost nicht direkt gedruckt, sondern über eine „E-POSTBUSINESS-BOX“, die der Auftragnehmer dem Auftraggeber zur Verfügung stellt, versendet.
Dabei kann zwischen elektronischer Zustellung und physischer Zustellung gewählt werden. An die Adressaten, die eine elektronische Zustellung ermöglicht haben, also schon eine E-Postbriefadresse besitzen und diese öffentlich gemacht haben, wird das Dokument elektronisch übermittelt, andernfalls ausgedruckt, kuvertiert und auf dem herkömmlichen Postweg (E-Postbrief) übermittelt.
Der TLfDI teilte dem Landratsamt mit, dass er dieses Verfahren wie auch das Verfahren De-Mail aus datenschutzrechtlicher Sicht grundsätzlich als kritisch ansieht, da nicht ausgeschlossen werden kann, dass der Inhalt der Schreiben dem Auftragnehmer zur Kenntnis gelangt.
Analog der Nutzung von De-Mail, gilt auch hier, dass bei Verfahren, in denen personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, verarbeitet werden, zusätzlich eine Ende-zu-Ende-Verschlüsselung einzusetzen ist.

Sofern die Behörde Hortgebührenbescheide versenden würde, könnte daraus die Adresse und die Höhe des zu leistenden Hortbeitrags erfasst werden. Hieraus ließen sich Rückschlüsse auf die Einkommenssituation des betroffenen Haushalts ziehen.
Bei dem vorgelegten Entwurf des Vertrages zur Datenverarbeitung im Auftrag handelte es sich zudem um einen Standardvertrag nach § 11 Bundesdatenschutzgesetz, der zwar den inhaltlichen Vorgaben des § 8 Thüringer Datenschutzgesetz (ThürDSG) entspricht, jedoch keine ausdrückliche Bezugnahme auf das ThürDSG beinhaltete. Sind auf den Auftragnehmer die Bestimmungen des ThürDSG nicht anwendbar, ist der Auftraggeber gemäß § 8 Abs. 6 Satz 1 ThürDSG verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des ThürDSG befolgt. Insofern forderte der TLfDI gegenüber dem Landratsamt, in die Ausgestaltung des Vertrages mindestens noch eine Regelung aufzunehmen, wonach § 8 ThürDSG auf das Auftragsdatenverarbeitungsverhältnis anzuwenden ist.

Bei Verfahren, in denen personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, verarbeitet werden, ist auch bei der Nutzung vom E-POSTBRIEF zusätzlich eine Ende-zu-Ende-Verschlüsselung einzusetzen. Dies gilt analog für die Nutzung von De-Mail. Sofern öffentliche Stellen einen Vertrag über eine Datenverarbeitung im Auftrag mit einer nicht-thüringischen Stelle schließen wollen, haben sie nach § 8 Abs. 6 Satz 1 ThürDSG vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des ThürDSG befolgt.

5.52 Wie viel Arbeitszeit braucht der Datenschutzbeauftragte?

Der Datenschutzbeauftragte einer Stadtverwaltung wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Unterstützung. Nachdem der Amtsvorgänger 30 % seiner Arbeitszeit für die Aufgaben des Datenschutzbeauftragten nach § 10a Thüringer Datenschutzgesetz (ThürDSG) zur Verfügung hatte und wegen nicht zufriedenstellender Aufgabenerfüllung abgelöst wurde, konnte sein Nachfolger erst mal für ein halbes Jahr 90 % seiner Arbeitszeit auf die Einarbeitung und Aufarbeitung der liegen gebliebenen Aufgaben aufwenden. Damit war es aber nach Auffassung des neuen Datenschutzbeauftragten noch nicht getan, um ein akzeptables Datenschutzniveau zu erlangen

und aufrechtzuerhalten. Das Anliegen war, diesen prozentualen Anteil der Arbeitszeit für den internen Datenschutz auch weiterhin zu erhalten, um nicht nur die aktuellen dringlichen Aufgaben zu erledigen, sondern auch frühzeitige Informationen erarbeiten und Schulungen für die Mitarbeiter der Stadtverwaltung anbieten zu können.
Der Oberbürgermeister, dem der Datenschutzbeauftragte nach § 10a ThürDSG direkt zu unterstellen ist, beauftragte nun den Fachdienst Personal und Organisation, um feststellen zu lassen, wieviele Arbeitszeitanteile für die Aufgabe Datenschutz benötigt würden. Dieser Fachdienst entwarf einen umfangreichen Fragebogen, in dem sich der Datenschutzbeauftragte für die Reihenfolge der Bearbeitung, den langen Zeitraum etc. rechtfertigen und seine jeweilige Tätigkeit genau auflisten sollte. Darüber hinaus sollte er zunächst für mehrere Wochen aufschreiben, womit er sich den ganzen Tag beschäftige (Kennzahl, Fallzahl, Sachverhalt, Abfolge der Tätigkeiten, Beginn, voraussichtliche Fertigstellung und Bearbeitungsdauer etc.).
Zu dem Ansinnen des Oberbürgermeisters führte der TLfDI aus, dass es der öffentlichen Verwaltung grundsätzlich zusteht, Organisationsuntersuchungen durchzuführen, um daraus Erkenntnisse für Organisationsfestlegungen zu treffen. Die Aufforderung zur Protokollierung der Tätigkeit des Datenschutzbeauftragten für den Zeitraum von mehreren Wochen stieß aus Sicht des TLfDI jedoch auf erhebliche Bedenken in Bezug auf die Stellung des Datenschutzbeauftragten nach § 10a ThürDSG.
Abgesehen davon, dass der Datenschutzbeauftragte nach § 10a Abs. 2a und Abs. 5 ThürDSG eine besondere Verschwiegenheitsverpflichtung hat und deshalb Sachverhalte umfangreich zu anonymisieren sind, damit keine Rückschlüsse auf die betroffenen Personen auch innerhalb der Stadtverwaltung ermöglicht werden, hat der Gesetzgeber dem Datenschutzbeauftragten eine besondere Stellung zugeschrieben. Er ist gemäß § 10a Abs. 2 ThürDSG in dieser Funktion dem Leiter der Daten verarbeitenden Stelle unmittelbar zu unterstellen und hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. In dieser Eigenschaft als Datenschutzbeauftragter ist er nicht weisungsgebunden.
Diese Weisungsfreiheit in der fachlichen Aufgabenerfüllung bedeutet allerdings nicht, dass die verantwortliche Stelle im Rahmen ihrer Dienstaufsicht nicht befugt wäre, sich zu vergewissern, ob der Beauftragte ordnungsgemäß seiner Aufgabe nachkommt (so auch Simi-

tis, Kommentar zum BDSG, zu § 4f Rn. 125). Die Protokollierung seiner Tätigkeit kann eine Überprüfung der Aufgabenerfüllung des Datenschutzbeauftragten durch die hierzu beauftragte Personalverwaltung darstellen. Bei einer minutiösen Aufschreibung sämtlicher Tätigkeiten entsteht jedoch eine vollständige Leistungs- und Verhaltenskontrolle – hier einer einzelnen Person –, die im Hinblick auf die direkte Unterstellung unter den Leiter der öffentlichen Stelle und die nicht weisungsgebundene Aufgabenwahrnehmung in dieser Intensität nicht zu rechtfertigen ist. Die Weisungsungebundenheit der bestellten Person bedingt auch, dass der Datenschutzbeauftragte nicht durch (auch zeitlich befristete) Belastung mit anderen Aufgaben (hier die Selbstaufschreibung) praktisch daran gehindert wird, den gesetzlichen Aufgaben nachkommen zu können. Zumindest für die Dauer der Untersuchung wird damit Einfluss auf die Tätigkeit des Datenschutzbeauftragten genommen, die mit seiner besonderen Stellung nicht vereinbar ist.
Offenbar war der Oberbürgermeister einsichtig, denn der Datenschutzbeauftragte machte von dem Angebot des TLfDI, erforderlichenfalls zu intervenieren, keinen Gebrauch.

Dem behördlichen Datenschutzbeauftragten (bDSB) kommt nach § 10a ThürDSG eine nicht zu unterschätzende Aufgabe und Stellung zu. Er ist in Erfüllung seiner gesetzlichen Aufgaben nicht weisungsgebunden. Neben den notwendigen Fachkenntnissen muss der Datenschutzbeauftragte auch die erforderliche Arbeitszeit zur Verfügung haben, damit er seinen Aufgaben nachkommen kann. Er darf ebenso wenig wie andere Beschäftigte einer vollständigen Leistungs- und Verhaltenskontrolle unterzogen werden und damit in der Ausübung seiner Aufgabe be- und gehindert werden.

5.53 Dürfen Stadtratsmitglieder die Gehälter der kommunalen Bediensteten überprüfen?

Der Stadtrat einer Stadt in Thüringen beschloss zu überprüfen, welche persönlichen Zulagen in welcher Höhe an welche kommunale Bedienstete auf welcher Grundlage durch die Stadt gezahlt werden. Da damit Beschäftigtendaten verarbeitet werden sollten, bat der Bürgermeister den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Hinweise zum Umgang mit den Personalaktendaten der Mitarbeiter der Stadtverwal-

tung im Zusammenhang mit der Rechnungsprüfung und auch zur Möglichkeit der Auskünfte aus bzw. der Einsicht in die Personalakten für Stadträte. Der TLfDI hat hierzu Folgendes ausgeführt:
Die Verarbeitung personenbezogener Daten ist nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nur dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Thüringer Datenschutzgesetz ist jedoch nach § 2 Abs. 3 ThürDSG subsidiär, wenn eine so genannte bereichsspezifische Regelung vorliegt. Die Thüringer Kommunalordnung (ThürKO) als Spezialgesetz enthält jedoch keine Erlaubnisnorm zur Verarbeitung von Mitarbeiterdaten durch den Stadtrat. Insoweit ist zunächst auf § 33 ThürDSG zurückzugreifen. Danach sind für das Verarbeiten oder Nutzen von personenbezogenen Daten über Angestellte, Arbeiter und Auszubildende in einer öffentlichen Stelle die dienstrechtlichen Vorschriften (§§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG) anzuwenden. Für (Kommunal-) Beamte gelten diese Vorschriften unmittelbar. Hier gilt der Grundsatz des § 80 Abs. 1 ThürBG, nach dem Zugang zu Personaldaten nur Beschäftigte (nicht Stadtratsmitglieder) haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist.
Nach § 80 Abs. 2 Satz 2 ThürBG haben Zugang ferner die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse nur auf diesem Weg und nicht durch Auskunft aus der Personalakte gewinnen können. Für andere Personen, also für Stadtratsmitglieder als Dritte, besteht keine Vorlage- oder Auskunftsmöglichkeit. Den Mitgliedern des Stadtrats und den Ausschüssen stehen jedoch nach der Rechtsprechung (VG Meiningen, Urteil vom 20. September 2011 – 2 K 303/10 Me- und Thüringer Oberverwaltungsgericht, Urteil vom 14. November 2013 – 3 KO 900/11-, juris) allgemeine Informationsrechte nach § 24 Abs. 1 ThürKO zu. Nach § 29 Abs. 3 ThürKO ist der Bürgermeister oberste Dienstbehörde der Beamten der Gemeinde und Dienstvorgesetzter der Gemeindebediensteten. Für die in § 29 Abs. 3 Satz 3 Nr. 1 und 2 ThürKO genannten Personalentscheidungen (Ernennung, Abordnung, Versetzung, Versetzung in den Ruhestand und Entlassung der Beamten des gehobenen und höheren Dienstes sowie Einstellung, Höhergruppierung und Entlassung von Angestellten mit vergleichbarer Vergütung) bedarf es der Zustim-

mung des Gemeinderats oder des zuständigen Ausschusses. Die Gewährung von Zulagen ist hier nicht konkret genannt. Insoweit hat der Bürgermeister in Wahrnehmung seiner Fürsorgepflicht für die betroffenen Beschäftigten mit Zulagen zunächst die Personalaktendaten vor unbefugter Einsicht zu schützen.
Eine Befugnis zur Offenbarung der Personalaktendaten gegenüber Stadträten besteht jedoch dann, wenn das allgemeine Informationsrecht auch personenbezogene Daten von Bediensteten umfassen muss, weil sonst die Kontrollfunktion der Stadträte nicht ausgeübt werden könnte. In einem solchen Fall ist das Kontrollrecht mit den schützenswerten Interessen der betroffenen Bediensteten abzuwägen. Im Rahmen dessen ist zu prüfen, ob zur Ausübung der Kontrollrechte durch die Stadtratsmitglieder oder den Ausschuss anonymisierte Angaben ausreichen. Sollte dies nicht der Fall sein, ist abzustufen, ob eine personenbezogene Auskunft für die Aufgabenerfüllung ausreicht, was in den meisten Fällen zutreffend sein sollte. Sollte im Einzelfall die Einsicht in Personalaktendaten begehrt werden, ist dies nach Auffassung des TLfDI auf die für die Aufgabenerfüllung zwingend erforderlichen Angaben zu beschränken.
Aber auch im Falle der Auskunft über personenbezogene Daten sind flankierende Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechts der Betroffenen zu treffen. Die personenbezogenen Daten dürfen daher nur in nicht-öffentlicher Sitzung (vgl. Thüringer Oberverwaltungsgericht, Urteil vom 14. November 2013 – 3 KO 900/11) unter Hinweis auf die Zweckbindung zur konkreten Aufgabenerfüllung zur Kenntnis gegeben und seitens der Empfänger nicht für andere Zwecke genutzt werden (siehe dazu Nr. 5.40).

Das Kontroll- und Prüfungsrecht eines Stadtrats kann sich auch auf die Gehälter der kommunalen Bediensteten beziehen. Die erforderlichen Beschäftigtendaten aus den Personalakten der Betroffenen müssen hierzu zur Verfügung gestellt werden. Mit einem generellen Zugang zur Personalakte ist dies jedoch nicht verbunden. In der Regel reichen anonymisierte Angaben für die Aufgabenerfüllung des Stadtrats aus. Bei besonderem Klärungsbedarf im Einzelfall ist abzuwägen, welche konkreten personenbezogenen Informationen zu einzelnen betroffenen Mitarbeitern dem Stadtrat vorgelegt werden können. Eine personenbezogene Erörterung darf nur in nicht-öffentlicher Sitzung erfolgen.

5.54 Streaming me softly? – Der Öffentlichkeitsgrundsatz in der ThürKO erfasst noch immer keine Live-Übertragung von Stadtratssitzungen

Im Mai 2015 startete die Landesbeauftragte für den Datenschutz in Niedersachsen eine Umfrage unter den deutschen Datenschutzbehörden, um zu klären, ob bzw. in welchen Bundesländern Bild- und Tonaufzeichnungen von öffentlichen Stadtratssitzungen mit dem Ziel der Veröffentlichung üblich bzw. gesetzlich geregelt sind. Die gesammelten Erkenntnisse sollten dann in einer allgemeinen Übersicht zusammengefasst werden.
Bereits in dem Tätigkeitsbericht 2011/2012 hatte der niedersächsische Datenschutzbeauftragte sich zu der Thematik eindeutig positioniert und hauptsächlich auf mangelnde gesetzliche Grundlagen hingewiesen, um im Ergebnis eine generelle Aufzeichnung oder einen Live-Stream abzulehnen. Dazu griff sie auch die Argumentation des Bundesverwaltungsgerichts (vgl. Urteil vom 3. August 1990, Aktenzeichen 7 C 14/90) auf, wonach zu befürchten sei, dass sich weniger wortgewandte Sitzungsteilnehmer zu sehr exponiert fühlen, als dass sie im Bewusstsein einer Aufzeichnung oder Live-Übertragung überhaupt noch frei und ungehemmt an der Sitzung teilnehmen und an der Beschlussfassung mitwirken könnten.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) teilte seiner niedersächsischen Kollegin mit, dass es in Thüringen derzeit keine Rechtsgrundlage in der Thüringer Kommunalordnung (ThürKO) für solche Aufzeichnungen oder Übertragungen gibt und verwies auf seinen eigenen Tätigkeitsbericht 2012/2013, in dem er ab Seite 95 ff. zur Live-Übertragung von Sitzungen eines Stadtrates Stellung bezogen hatte. Dort hatte der TLfDI auch die „Erfurter Lösung“ vorgestellt, die sich übrigens bis heute bewährt hat. Der TLfDI ist gespannt zu erfahren, wie die übrigen Datenschutzbeauftragten der Länder dieses Modell beurteilen.
Nach § 40 Abs. 1 Thüringer Kommunalordnung (ThürKO) sind Sitzungen des Gemeinderats grundsätzlich öffentlich durchzuführen. Dieses Gebot ist jedoch schon dann gewahrt, wenn ein ausreichend großer Sitzungsraum für den Normalbürger zumutbar erreichbar ist, zu dem jedermann im Rahmen des hierfür zur Verfügung stehenden Platzes in der Reihenfolge des Eintreffens freien Zugang hat. Daher besteht keine Berechtigung für eine Übertragung des Sitzungsverlaufs mit elektronischen Medien. Folglich können aus § 40 Abs. 1

ThürKO keine weitergehenden Befugnisse für Eingriffe in das Recht auf informationelle Selbstbestimmung der anwesenden Personen abgeleitet werden, als dass die anwesenden Zuhörer sich gegebenenfalls Notizen machen und im Anschluss an die Sitzung in der Presse berichtet wird. Aus kommunalrechtlicher Sicht ist zu beachten, dass es nach der Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 3. August 1990, 7 C 14/90) im öffentlichen Interesse liegt, wenn die Willensbildung im Rat ungezwungen, freimütig und in aller Offenheit erfolgt. Nach dieser Entscheidung kann durch eine Tonbandaufzeichnung eines Journalisten diese Willensbildung dadurch beeinträchtigt werden, dass „insbesondere in kleineren und ländlichen Gemeinden weniger redegewandte Ratsmitglieder durch das Bewusstsein des Tonmitschnitts ihre Spontanität verlieren, ihre Meinung nicht mehr ‚geradeheraus' vertreten oder schweigen, wo sie sonst gesprochen hätten". Diese Grundsätze hat das Bundesverwaltungsgericht für eine zulässige Einschränkung der Pressefreiheit aufgestellt. Sie müssen erst recht gelten, wenn im Rahmen der Abwägung das Grundrecht der Pressefreiheit nicht mit einzubeziehen ist, weil die Kommune selbst derartige Aufzeichnungen und Übertragungen vornimmt. Deshalb liegt es immer in der Sitzungs- und Hausordnungsbefugnis des Vorsitzenden, im Einzelfall zu entscheiden, ob durch die beabsichtigte Aufzeichnung dieses öffentliche Interesse an einer unbeeinträchtigten Willensbildung verletzt würde und daher zu untersagen ist. Diese Grundsätze kommen erst recht bei Bildaufnahmen zum Tragen, die mittels elektronischer Medien wie dem Internet einer weltweiten Öffentlichkeit zugänglich gemacht werden. Somit existieren nach derzeitiger Rechtslage keine Vorschriften direkt in der Thüringer Kommunalordnung (ThürKO), die eine Publikation von Gemeinderatssitzungen erlauben oder anordnen.

Da der TLfDI Verständnis für das Ansinnen der Kommunen hat, die Arbeit in den Gemeinderatssitzungen noch transparenter zu gestalten, hatte er bereits im Jahr 2013 einen Gesetzentwurf zur Änderung der ThürKO zwecks Verbesserung der Transparenz von Gemeinderatssitzungen ausgearbeitet. Diesen Gesetzentwurf hatte er an die Fraktionen des Thüringer Landtags zur Prüfung weitergegeben. Weder in der abgelaufenen 5. Wahlperiode noch in der im Jahr 2014 begonnenen 6. Wahlperiode hat der Thüringer Landtag die Vorschläge des TLfDI zur datenschutzkonformen Live-Übertragung von Stadtratssitzungen im Internet aufgegriffen und die ThürKO entspre-

chend angepasst. Der TLfDI wird daher zu gegebener Zeit erneut seine Vorschläge zu dieser wichtigen Thematik an die Fraktionen des Landtags übermitteln.
Der Gesetzentwurf orientierte sich an den Vorgaben der Entscheidung des Oberverwaltungsgerichts (OVG) Saarlouis (Urteil vom 30. August 2010, 3B 203/10). Danach sind Medienunternehmen unter der Voraussetzung, dass das Persönlichkeitsrecht der bei der Sitzung anwesenden Personen nicht durch die Berichterstattung beeinträchtigt wird, berechtigt, von öffentlichen Sitzungen in Bild und Ton zu berichten. Unter diesen Voraussetzungen ist auch ein Live-Mitschnitt einer öffentlichen Stadtratssitzung für das Internet als zulässig anzusehen. Ein Beispiel einer solchen Fallkonstellation stellt die Übertragung öffentlicher Sitzungen des Stadtrats Erfurt in der Verantwortlichkeit der Zeitungsgruppe Thüringen aufgrund eines Bewilligungsbescheids der Stadtverwaltung Erfurt dar. Hierbei gelten neben dem Datenschutz auch presse- bzw. rundfunkspezifische Rechte. Das Persönlichkeitsrecht der bei der Sitzung anwesenden Personen, wie Stadtratsmitglieder, Besucher und städtische Beschäftigte, wird aufgrund spezieller Regelungen der Geschäftsordnung des Stadtrats, die auf der Homepage der Stadt Erfurt veröffentlicht wurden, garantiert. So ist vor der jeweiligen Stadtratssitzung die Kamera so zu positionieren, dass nur der jeweilige Redner am Rednerpult und das Präsidium hinter dem Rednerpult aufgezeichnet werden. Auch haben die beteiligten Personen die Möglichkeit, ihrer Aufnahme zu widersprechen. Im Ergebnis bestehen daher keine datenschutzrechtlichen Bedenken gegen diese „Erfurter Lösung“.

Nicht zum ersten Mal soll an dieser Stelle ein kleiner Appell erfolgen: Das Recht muss sich konsequent an neue gesellschaftliche und technologische Entwicklungen anpassen. Insbesondere muss allgemeines und spezielles Verfahrensrecht an neue Kommunikationsmittel und Kommunikationsgewohnheiten angepasst werden. Dies gilt auch für die ThürKO: Der TLfDI hatte bereits vor drei Jahren einen Vorschlag für eine Regelung unterbreitet, wie Sitzungen des Gemeinderats im Internet live und datenschutzkonform übertragen werden können. Bislang griff der Gesetzgeber diesen Vorschlag nicht auf. Der TLfDI übt sich daher auch auf dieser Baustelle im Bohren dicker Bretter.

5.55 Verarbeitung von Einkommensdaten zur Festsetzung von Hortgebühren

In einer Eingabe beschwerten sich Eltern beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den Umfang der Anforderung von Unterlagen zur Festsetzung der Hortgebühren in der Stadt Jena. Unter anderem wurden auf einem Erhebungsbogen die Telefonnummer, die E-Mail-Adresse, der Beschäftigtenstatus, Auskünfte über die Einkommensverhältnisse sowie ein Kontoauszug zum Bezug von Kindergeld erhoben. Da zum Zeitpunkt der Erhebung ab einer bereinigten Einkommenshöhe von mehr als 2.500 Euro ohnehin der Hortgebühren-Höchstsatz festgelegt wurde, bestand aus datenschutzrechtlicher Sicht keine Erforderlichkeit dafür, diese Angabe bei allen Betroffenen zu erheben. Der Grund für den Nachweis eines Kindergeldbezugs war ebenfalls zunächst nicht einsichtig. Der TLfDI wandte sich deshalb an die Stadtverwaltung und bat um Prüfung und Auskunft zu dieser Datenerhebung. Die Stadtverwaltung nahm die Nachfrage des TLfDI zum Anlass, die bisher verwendeten Formulare zu überarbeiten und den zu erhebenden Datenumfang an die Vorschriften der Thüringer Hortkostenbeteiligungsverordnung und die städtische Hortkostenbeteiligungssatzung anzupassen. In dem neuen Auskunftsbogen werden die Telefonnummer und die E-Mail-Adresse als freiwillige Angaben gekennzeichnet. Ferner wurde klargestellt, dass der Beschäftigtenstatus nur anzugeben ist, wenn das bereinigte Einkommen unter 2.500 Euro monatlich liegt. Ebenso entfallen dann die für eine Ermäßigung der Hortgebühren ansonsten beizufügenden Einkommensnachweise. Ab dem zweiten kindergeldberechtigten Kind im Haushalt bleibt es dabei, dass Nachweise über die Kindergeldzahlung eingereicht werden müssen. Der Grund dafür ist, dass unabhängig von der Einkommenshöhe nach der Thüringer Verordnung über eine Hortkostenbeteiligung und der Hortkostenbeteiligungssatzung grundsätzlich eine Ermäßigung der Gebühren um 25 % für jedes weitere Kind einer Familie erfolgt. Die Stadtverwaltung wies darauf hin, dass auf dem Kontoauszug über die Kindergeldzahlung von den Betroffenen alle anderen Daten geschwärzt werden können. Im Ergebnis entspricht das geänderte Anforderungsschreiben der Stadt Jena nunmehr den datenschutzrechtlichen Vorschriften.

Bei der Berechnung der festzusetzenden Hortgebühren dürfen von einer Gemeinde nur die unbedingt zur Antragsbearbeitung erforderlichen Daten erhoben werden. Falls Kontoauszüge als Nachweis beizufügen sind, dürfen alle nicht erforderlichen Angaben auf diesen Auszügen unkenntlich gemacht werden.

5.56 Datenübermittlung im Verwaltungsverfahren

Im Berichtszeitraum hatte sich ein Ehepaar als Beschwerdeführer mit folgendem Sachverhalt an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt:
Sie hätten eine Dienstleisterfirma wegen zahlreicher illegaler Handlungen beim Landratsamt Schmalkalden-Meiningen angezeigt. Dabei hätten sie das Landratsamt gebeten, ihre personenbezogenen Daten nicht weiterzugeben. Daraufhin habe das Landratsamt den Beschwerdeführern erklärt, nur dann tätig werden zu können, wenn es ihre personenbezogenen Daten dem Angezeigten, also der Dienstleisterfirma, mitteilen könnte.
Der TLfDI bat das Landratsamt Schmalkalden-Meiningen um eine Stellungnahme zum oben genannten Tatbestand und forderte es auf, die Rechtsgrundlage zu nennen, die ein Tätigwerden des Landratsamtes zwingend von der Benennung personenbezogener Daten der Beschwerdeführer abhängig macht.
Außerdem fragte der TLfDI nach, warum eine Übermittlung personenbezogener Daten der Beschwerdeführer im konkreten Fall erforderlich sei.
Das Landratsamt Schmalkalden-Meiningen erklärte dem TLfDI daraufhin, dass es in seiner Anordnung an die Dienstleisterfirma (als Störer) – die aufgrund der Anzeige der Beschwerdeführer erfolgte – keine Zeugen benannt habe; dies werde sich aber in einem zu erwartenden Widerspruchsverfahren zur erfolgreichen Widerspruchsbegründung nicht vermeiden lassen.
Als Rechtsgrundlage für die Benennung von Zeugen verwies die Behörde auf § 26 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG), der das Beweismittel der Vernehmung von Zeugen regelt. Danach ist es den Behörden im Verwaltungsverfahren in den Grenzen ihres pflichtgemäßen Ermessens überlassen, Beweise zu erheben.
Eine Mitwirkungspflicht der Beteiligten besteht dabei grundsätzlich nicht. Eine Einvernahme von Zeugen geschieht freiwillig und kann –

von wenigen Ausnahmen abgesehen – nicht von der Behörde erzwungen werden.
Vorliegend war eine Mitwirkungshandlung insoweit erforderlich, weil ohne die Anzeige der Beschwerdeführer das in Rede stehende Verfahren gar nicht in Gang gesetzt worden wäre.
Von diesem Mitwirken der Beschwerdeführer in dieser Angelegenheit zu unterscheiden ist die Bekanntgabe ihrer Namen gegenüber dem Adressaten des Bescheides.
Dazu bestimmt § 39 ThürVwVfG – Begründung des Verwaltungsaktes – Folgendes:
„Ein schriftlicher oder elektronischer sowie ein schriftlich oder elektronisch bestätigter Verwaltungsakt ist mit einer Begründung zu versehen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben. Die Begründung von Ermessensentscheidungen soll auch die Gesichtspunkte erkennen lassen, von denen die Behörde bei der Ausübung ihres Ermessens ausgegangen ist.“
Die Mitteilung des Namens von Anzeigenerstattern ist dort nicht vorgesehen und damit datenschutzrechtlich grundsätzlich unzulässig.
In einem weiteren Schreiben bat der TLfDI das Landratsamt deswegen, nochmals zu prüfen, ob eine namentliche Nennung der Beschwerdeführer im weiteren Verfahren erforderlich sei und ob ein anderes, gleichwertig geeignetes Beweismittel im Sinne des § 26 ThürVwVfG in Betracht käme.
Das Landratsamt Schmalkalden-Meiningen erklärte daraufhin dem TLfDI, dass die Beschwerdeführer sich damit einverstanden erklärt hätten, als Zeugen zur Verfügung zu stehen. Das Landratsamt hatte aber von der Möglichkeit, die Beschwerdeführer als Zeugen einzusetzen, wie dargelegt, keinen Gebrauch gemacht. Das wies das Landratsamt gegenüber dem TLfDI auch nach, indem es seine bisherige Korrespondenz in der Angelegenheit offenlegte.
In der Regel überwiegt das Interesse des Anzeigenerstatters, anonym zu bleiben, das Interesse des Bescheidadressaten auf Nennung dessen Namens, sodass grundsätzlich – wie oben ausgeführt – die Übermittlung des Namens im Bescheid ohne dessen Einverständnis unzulässig ist.
Im Ergebnis konnte der TLfDI nicht feststellen, dass das Landratsamt Schmalkalden Meiningen personenbezogene Daten der Beschwerdeführer rechtswidrig verarbeitet hatte. Die Beschwerde war daher unbegründet.

§ 26 Abs. 1 ThürVwVfG ermöglicht den Behörden, in einem Verwaltungsverfahren Beweise zu erheben. Dazu gehört nach § 26 Abs. 1 Nr. 2 ThürVwVfG auch die Vernehmung von Zeugen. Bei der Sachverhaltsermittlung sind die Behörden deswegen befugt, nach pflichtgemäßem Ermessen unter anderem auch Zeugen zu vernehmen und somit personenbezogene Daten zu verarbeiten. Diese Daten können der Behörde unter anderem dazu dienen, Bescheide zu erlassen.

5.57 Pfändung nur bei Kenntnis der Bankverbindung zulässig!

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag im Berichtszeitraum eine Beschwerde vor, die folgenden Sachverhalt umfasste:
Gegen den Beschwerdeführer sei eine Pfändungs- und Einziehungsverfügung der Stadtverwaltung Eisfeld ergangen. Die Stadtverwaltung habe ihm einen entsprechenden Bescheid über eine Kontopfändung bei der VR-Bank Südthüringen zugestellt. Der Beschwerdeführer habe im Gegensatz zu seiner Ehefrau jedoch gar kein Konto bei der VR-Bank Südthüringen unterhalten. Der von diesem Verwaltungshandeln betroffene Beschwerdeführer begehrte von der Stadtverwaltung Eisfeld Auskunft, woher ihre Kenntnis über das vermeintliche Konto des Beschwerdeführers bei der VR-Bank Südthüringen stamme. Diese Auskunft sei dem Beschwerdeführer mehrfach telefonisch von der Stadt Eisfeld verweigert worden.
Der TLfDI bat die Stadtverwaltung Eisfeld um eine Stellungnahme zu der geschilderten Sach- und Rechtslage. Insbesondere interessierte ihn, aufgrund welcher Rechtsgrundlage die Stadtverwaltung Eisfeld die VR-Bank über die geplante Kontopfändung beim Beschwerdeführer in Kenntnis gesetzt habe und inwieweit diese Mitteilung für ihr Handeln in dieser Angelegenheit erforderlich gewesen sei.
Darüber hinaus wollte der TLfDI wissen, ob die Stadt Eisfeld dem Beschwerdeführer die Auskunft darüber verweigert habe, woher sie die Kenntnis über ein angebliches Konto des Beschwerdeführers bei der VR-Bank erlangt habe.
Der Vorwurf des Beschwerdeführers, ihm sei die Auskunft darüber verweigert worden, hat sich nach den Recherchen des TLfDI nicht bestätigt. Denn die Stadt Eisfeld hatte gegenüber dem Beschwerde-

führer schriftlich Auskunft erteilt, woher ihr Wissen um das vermutliche Konto des Beschwerdeführers stammte.
Zum Beweis dafür überließ die Stadtverwaltung dem TLfDI ein Schreiben, das sie seinerzeit an den Beschwerdeführer übersandt hatte. Darin hatte die Stadt Eisfeld dem Beschwerdeführer unter anderem mitgeteilt, dass das Auskunftsersuchen gegenüber der VR-Bank Südthüringen lediglich auf Erfahrungswerten beruhe, da dieses Institut erfahrungsgemäß in der Region häufig als Bank in Erscheinung träte. Eine unzulässige Verwendung personenbezogener Daten seitens der Stadtverwaltung Eisfeld wäre damit aber nicht verbunden gewesen.
Die Stadtverwaltung Eisfeld konnte jedoch keine Rechtsgrundlage für die von ihr gegenüber der Bank begehrte Übermittlung von Daten des Beschwerdeführers benennen.
Die Erfahrung, dass dieses Institut in dieser Region oft als Hausbank auftritt, rechtfertigt es nicht, ohne Rechtsgrundlage – nur aufgrund dieser Erkenntnis – „ins Blaue“ hinein das Kreditinstitut über eine geplante Kontopfändung eines ihrer Kunden in Kenntnis zu setzen. „Verwaltungserfahrungen“ legitimieren keine Anfrage einer Behörde nach personenbezogenen Kontodaten bei einer nichtöffentlichen Stelle.
Im Ergebnis handelte es sich vorliegend um einen Verstoß gegen § 22 Thüringer Datenschutzgesetz (ThürDSG). Die Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle – eine solche Stelle stellt die VR-Bank Südthüringen dar –ist nur zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§ 4 Abs. 1 ThürDSG). Eine Regelung oder Einwilligung des Beschwerdeführers, die die Behörde ermächtigt, der VR-Bank Südthüringen personenbezogene Daten des Beschwerdeführers zu übermitteln, lag mithin nicht vor.
Der TLfDI hat die Stadtverwaltung Eisfeld über seine Bewertung der Sach- und Rechtslage in Kenntnis gesetzt und sie aufgefordert, künftig den Belangen des Datenschutzes in gleichgelagerten Fällen Rechnung zu tragen. Beispielsweise könne der Schuldner unter Fristsetzung zukünftig zunächst aufgefordert werden, seine Bankverbindung zum Zwecke der Kontenpfändung der Stadtverwaltung bekanntzugeben; hiermit verbunden sein könnte der Hinweis, dass andernfalls einen Pfändung durch den Gerichtsvollzieher erfolgen wird.

Der TLfDI forderte die Stadtverwaltung Eisfeld auf, ihm mitzuteilen, wie sie die betreffenden Verfahrensabläufe im Sinne der Einhaltung der datenschutzrechtlichen Vorschriften künftig zu verändern gedenke. Im nächsten Datenschutzbericht wird der TLfDI über die Entwicklung in dieser Angelegenheit berichten.

Die Vermutung, dass ein Kostenschuldner eines Verwaltungsaktes bei einem Kreditinstitut eine Bankverbindung unterhält, berechtigt eine Behörde als Gläubiger dieser Forderung nicht, ein Kreditinstitut über seine Absicht einer Kontopfändung beim Kostenschuldner zu unterrichten. Lediglich bei sicherer Kenntnis der Bankverbindung des Kostenschuldners bei dem betreffenden Institut ist die Information über eine Kontopfändung aus datenschutzrechtlichen Gesichtspunkten gerechtfertigt.

5.58 Facebook weckt behördliche Überwachungsfantasien

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte im Berichtszeitraum Kenntnis davon, dass Mitarbeiter des Städtischen Ordnungsamtes Arnstadt im Auftrag ihres Amtsleiters Recherchen zur Erledigung folgender dienstlicher Aufgaben im sozialen Netzwerk Facebook durchführen sollten:

1. Präventive und kontrollierende Recherchen zu öffentlichen Vergnügungen im Straßenraum der Stadt Arnstadt zwecks Vorbereitung von Erlaubnis- bzw. Auflagenbescheiden nach § 42 Ordnungsbehördengesetz (OBG),
2. Erlangung von ordnungsbehördlich relevanten Hintergrundinformationen zu sozialen Gruppen und Initiativen im Stadtgebiet von Arnstadt,
3. Recherche zwecks Umsetzung / Ergreifung von Maßnahmen nach der Thüringer Prostitutionsverordnung und
4. lediglich mit „usw." bezeichnete etwaige weitere Aufgaben.

Zu dieser „Informationserlangung" via Facebook vertrat der TLfDI folgende datenschutzrechtliche Auffassung:

Bei einer Recherche einer öffentlichen Stelle in Facebook handelt es sich um eine Erhebung personenbezogener Daten ohne Mitwirkung

des Betroffenen im Sinne von § 19 Abs. 2 Satz 2 Thüringer Datenschutzgesetz (ThürDSG). Die Zulässigkeit einer solchen Datenerhebung setzt voraus, dass die Kenntnis der erhobenen Daten zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist (§ 19 Abs. 1 ThürDSG) und 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder 2. die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder 3. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (§ 19 Abs. 2 Satz 2 ThürDSG). Konkret ergab sich daraus folgende Wertung hinsichtlich der von der Stadt Arnstadt verfolgten Erhebungszwecke:

Zu 1. (Vorbereitung von Erlaubnis- bzw. Auflagenbescheiden nach § 42 OBG):
§ 42 OBG regelt die Veranstaltung von Vergnügungen. Nach § 42 Abs. 1 OBG hat, wer eine öffentliche Vergnügung veranstalten will, der zuständigen Stelle Art, Ort, und Zeit der Veranstaltung sowie die Zahl der zuzulassenden Teilnehmer spätestens eine Woche zuvor schriftlich anzuzeigen. § 42 Abs. 3 OBG regelt Veranstaltungen öffentlicher Vergnügungen, die einer Erlaubnis bedürfen und die Zuständigkeit der Erteilung einer solchen Erlaubnis. Ein Veranstalter, der nach § 42 Abs. 1 OBG der Stadtverwaltung die o. g. Pflichtangaben gemeldet hat, bedarf keiner Erlaubnis. Einer Erlaubnis bedarf es lediglich in Fällen des § 42 Abs. 3 OBG, z. B. wenn es sich um eine motorsportliche Veranstaltung handelt.
Da eine Stadtverwaltung durch die Anzeigeverpflichtung in ausreichendem Maße über Veranstaltungen in Kenntnis gesetzt wird, bestand aus der Sicht des TLfDI im konkreten Fall keine Notwendigkeit für eine zusätzliche Datenerhebung mittels einer Recherche in sozialen Netzwerken durch Mitarbeiter der Stadtverwaltung Arnstadt. Zu berücksichtigen war dabei auch die Möglichkeit, dass weitere personenbezogene Daten, ggf. auch von Dritten, die in keinem Zusammenhang mit der ordnungsbehördlichen Tätigkeit stehen, quasi als „Beifang“ hätten erhoben werden können. Im Ergebnis waren deshalb die beabsichtigten präventiven und kontrollierenden Facebook-Recherchen zu öffentlichen Vergnügungen nicht von § 19 Abs. 2 ThürDSG in Verbindung mit § 42 OBG gedeckt. Anderweitige Rechtsgrundlagen, die eine derartige Datenerhebung erlaubt hätten, waren für den TLfDI nicht ersichtlich.

Zu 2. (Erlangung relevanter Hintergrundinformationen zu sozialen Gruppen und Initiativen):
Für die „Erlangung ordnungsbehördlich relevanter Hintergrundinformationen“ (was auch immer das sein mag) zu sozialen Gruppen und Initiativen aufgrund von Facebook-Recherchen war eine geeignete Rechtsgrundlage aus Sicht des TLfDI ebenfalls nicht ersichtlich. Bedenklich erschien in diesem Zusammenhang insbesondere die unbestimmte Formulierung „Hintergrundinformationen“, die die Entscheidung, welche Daten konkret zu erheben wären, von der eigenverantwortlichen Beurteilung des recherchierenden Mitarbeiters abhängig machte. Im Ergebnis stand deshalb zu befürchten, dass dem auch in § 19 Abs. 2 Satz 2 Nr. 2 ThürDSG enthaltenen datenschutzrechtlichen Gebot der Erforderlichkeit im konkreten Fall nicht ausreichend Rechnung getragen worden wäre und daher zu befürchten war, dass personenbezogene Daten des Betroffenen und auch von Dritten im Übermaß erhoben worden wären.

Zu 3. (Umsetzung / Ergreifung von Maßnahmen nach der Thüringer Prostitutionsverordnung):
Die Thüringer Verordnung über das Verbot der Prostitution regelt die Zulässigkeit der Prostitution entsprechend der Gemeindegröße / Anzahl der Einwohner. Auch hier bestanden nach Einschätzung des TLfDI Zweifel an der Datenschutzkonformität einer diesbezüglichen Facebook-Recherche, da eine geeignete Rechtsgrundlage mangels Vorliegen der Voraussetzungen des § 19 Abs. 2 ThürDSG nicht ersichtlich war.

Zu 4. (als „usw.“ bezeichnete weitere Aufgaben):
Das ThürDSG verbietet grundsätzlich jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten, es sei denn, sie ist ausdrücklich gesetzlich erlaubt (Grundsatz des Verbots mit Erlaubnisvorbehalt, vgl. § 4 Abs. 1 ThürDSG).
Daraus ergab sich für den vorliegenden Fall, dass die offene Formulierung „usw.“ Raum ließ für weitere, nicht näher bezeichnete und damit ggf. unerlaubte Erhebungszwecke. Im Ergebnis genügte die Formulierung „usw.“ nicht den datenschutzrechtlichen Anforderungen.

Die datenschutzrechtliche Beurteilung des konkreten Sachverhalts hing darüber hinaus davon ab, ob die personenbezogenen Daten, die

das Ordnungsamt recherchieren sollte, öffentlich zugänglichen Quellen im Sinne von § 20 Abs. 2 ThürDSG entstammten. Kann auch ein nicht angemeldeter Nutzer bei Facebook personenbezogene Daten einsehen, so handelt es sich um öffentlich zugängliche Quellen. Hat ein Betroffener bei der Einrichtung einer Facebook-Seite seine Daten öffentlich zugänglich gemacht, ist nicht von einem schutzwürdigen Interesse an der Nicht-Nutzung dieser personenbezogenen Daten auszugehen.
Vom Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder wurde im Februar 2011 erörtert, welche Daten in sozialen Netzwerken als allgemein zugängliche Daten angesehen werden können. Im Ergebnis wurde übereinstimmend festgestellt, dass diejenigen Daten, die über allgemeine Suchmaschinen erschlossen werden können, allgemein zugängliche Daten sind.
Die Erhebung allgemein zugänglicher Daten aus sozialen Netzwerken durch Strafverfolgungs- und Gefahrenabwehrbehörden stellt zumindest dann einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, wenn dies zielgerichtet zu einer bestimmten oder bestimmbaren Person erfolgt. Als Rechtsgrundlage hierfür reichen in der Regel die Generalklauseln (§§ 161, 163 StPO, polizeiliche Generalklauseln) aus. §§ 161, 163 StPO finden gemäß § 46 Abs. 1 OWiG auch bei der Verfolgung von Ordnungswidrigkeiten Anwendung.
Zur Aufgabenerfüllung darf eine öffentliche Stelle jedoch grundsätzlich nicht selbst als privater Nutzer mit einem „Fake-Account“ in Facebook recherchieren und personenbezogene Daten erheben. Dies würde nicht zuletzt einen Verstoß gegen die Nutzungsbedingungen von Facebook darstellen. So fordert Facebook z. B. in seinen Nutzungsbedingungen Nr. 5 Pkt. 7 folgendes Verhalten:

„Wenn du Informationen von Nutzern erfasst, dann wirst du Folgendes tun: Ihre Zustimmung einholen, klarstellen, dass du (und nicht Facebook) ihre Informationen sammelst, und Datenschutzrichtlinien bereitstellen, in denen du erklärst, welche Informationen du sammelst und wie du diese verwenden wirst!“

Aber auch hinsichtlich der Umstände der Facebook-Recherche mittels dienstlicher PCs der Stadtverwaltung ergaben sich aus folgenden Gründen datenschutzrechtliche Bedenken:

Facebook installiert eine Reihe von Cookies, d. h. in einem solchen Falle auch auf den Dienst-PCs! Da Facebook seine tatsächliche Funktionalität derzeit noch nicht datenschutzrechtlich befriedigend transparent dargestellt hat, kann nicht ausgeschlossen werden, dass sämtliche besuchte Internet-Seiten und auch auf dem PC vorhandene Adressbücher mit den darin enthaltenen Kontaktadressen unbeteiligter Dritter heimlich durch Facebook erfasst werden. Dies stellt eine unzulässige Datenübermittlung dar.
Im Ergebnis riet der TLfDI dringend von der beabsichtigten Facebook-Nutzung ab. Die Stadt Arnstadt trug den Bedenken des TLfDI Rechnung und gab das Vorhaben auf.

Das ThürDSG schützt die personenbezogenen Daten des Einzelnen vor dem Zugriff öffentlicher Stellen schon recht weitgehend. Im Fall der Stadtverwaltung Arnstadt konnte der TLfDI jedenfalls keine Rechtsgrundlagen entdecken, die eine Datenerhebung durch städtische Mitarbeiter ohne Mitwirkung des Betroffenen erlaubten.

5.59 Durch und durch Datenschutz

Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis von möglichen datenschutzrechtlichen Verstößen der Stadt Nordhausen. Es stand der Verdacht im Raum, dass verschiedene Dokumente, die einen Personenbezug zu einem Beschwerdeführer aufwiesen, unberechtigt an Dritte weitergegeben bzw. veröffentlicht wurden.
Zur Sachverhaltsaufklärung wandte sich der TLfDI an den Oberbürgermeister der Stadtverwaltung Nordhausen und bat im Rahmen seiner Kontrollkompetenz nach § 37 Abs. 1 i. V m. § 38 Abs. 1 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) um eine Stellungnahme zu diesen Vorwürfen. Eine Antwort des Oberbürgermeisters blieb aus. Trotz nochmaliger Erinnerung seitens des TLfDI blieben die Fragen unbeantwortet. Der von der Stadt Nordhausen zwischenzeitlich beauftragte Rechtsanwalt teilte dann in einem Schreiben unter anderem mit, dass eine Stellungnahme derzeit nicht erfolgen würde. Diese Weigerung stellte einen Verstoß gegen die Pflicht der Stadtverwaltung Nordhausen dar, den TLfDI gemäß § 38 Abs. 1 Nr. 1 ThürDSG in der Erfüllung seiner Aufgaben zu unterstützen. Der TLfDI beanstandete gemäß § 39 Abs. 1 S. 1 ThürDSG förmlich diesen Datenschutzverstoß und unterrichtete hiervon das Landratsamt Nordhausen

als Kommunalaufsichtsbehörde und das Thüringer Innenministerium gemäß § 39 Abs. 1 Satz 2 ThürDSG.
Kurz darauf führte der TLfDI eine datenschutzrechtliche Kontrolle bei der Stadtverwaltung Nordhausen durch. Dabei stellte der TLfDI fest, dass seit dem Ausscheiden des vorherigen behördlichen Datenschutzbeauftragten (bDSB) aus dem Dienst die Stadt Nordhausen von Ende Oktober 2012 bis Mitte des Jahres 2014 über keinen rechtswirksam bestellten behördlichen Datenschutzbeauftragten nach § 10a ThürDSG verfügte. Weiterhin hatte die Stadt Nordhausen in einem Disziplinarverfahren einen Rechtsanwalt als externen Ermittlungsführer beauftragt und diesem sensible personenbezogene Daten übermittelt. Die Beauftragung eines Rechtsanwalts als externen Ermittlungsführer seitens der Stadt Nordhausen in einem Disziplinarverfahren stellte eine unzulässige Datenübermittlung an einen unberechtigten Dritten dar, die nicht durch § 22 ThürDSG gerechtfertigt war. Insbesondere kann § 28 Thüringer Disziplinargesetz (ThürDG) in Verbindung mit § 21 Abs. 1 Nr. 1 und § 20 Abs. 2 Nr. 1 ThürDSG in diesem Fall nicht zur Rechtfertigung einer Datenübermittlung herangezogen werden. Bereits aus dem Wortlaut von § 28 Satz 2 ThürDG, aber auch nach Auffassung der Literatur, ergibt sich, dass Ermittlungsführer nur eine innerhalb des öffentlichen Dienstes stehende Person sein kann. Denn nur eine solche Person kann nach dem Wortlaut dieser Vorschrift als „Ermittlungsführer“ für die Dauer seiner Aufgabe „im Hauptamt entlastet“ werden. Für einen Rechtsanwalt als Ermittlungsführer – wie im vorliegenden Fall – läuft § 28 Satz 2 ThürDG gerade ins Leere.
Der TLfDI stellte weiter fest, dass in einer öffentlichen Sitzung des Hauptausschusses der Stadt Nordhausen der Oberbürgermeister Angaben über die Eröffnung eines Disziplinarverfahrens gemacht hatte. Diese Übermittlung der bis dahin nicht medienbekannten personenbezogenen Daten stellte einen Verstoß gegen § 40 Abs. 1 Thüringer Kommunalordnung (ThürKO) dar, da Personalangelegenheiten als Teil des vertraulich zu behandelnden persönlichen Bereichs des Einzelnen nicht Gegenstand einer öffentlichen Sitzung sein dürfen (siehe dazu Rücker/Dieter/Schmidt, ThürKO, Kommentar, § 40, Nr. 2.4, Seite 6).
Diese Verstöße beanstandete der TLfDI förmlich gemäß § 39 Abs. 1 S. 1 ThürDSG und unterrichtete hiervon das Landratsamt – Kommunalaufsicht – und das Thüringer Innenministerium gemäß § 39 Abs. 1 S. 2 ThürDSG.

Der Stadt Nordhausen versicherte, aufgrund des „regen“ Kontaktes mit dem TLfDI auf die Einhaltung der Datenschutzbestimmungen ein besonderes Augenmerk zu legen.

Der TLfDI musste in Nordhausen mehrere Male zu seinem schärfsten Schwert – der förmlichen Beanstandung gemäß § 39 Abs. 1 ThürDSG – greifen. Umso erfreulicher ist es, dass nunmehr seitens der Stadt ein besonderes Augenmerk auf den Datenschutz gelegt wird.

5.60 „Datenskandal“ bei den Kraftwerken Gera – personenbezogene Daten auf der Müllkippe

Im Berichtszeitraum hatte, laut einem Bericht des MDR, einer seiner Mitarbeiter zwei Festplatten auf einem Werkstoffhof in Gera gefunden. Der MDR informierte daraufhin in Erfurt den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da auf den gefundenen Festplatten zum Teil brisante Arbeitnehmerdaten seien. Der MDR, die Bild-Zeitung und zahlreiche andere Medien berichteten dann über den „Datenskandal bei den Kraftwerken Gera“.
Der TLfDI erhielt Zugang zu Kopien der aufgefundenen Festplatten und überprüfte diese auf das Vorhandensein personenbezogener Daten. Seine Prüfung ergab, dass es sich bei den aufgefundenen Festplatten um solche von zwei Mitarbeitern der Kraftwerke Gera GmbH handelte und dass neben dienstlichen Berichten, Bestellungen und Anweisungen auch Gehalts-, Gesundheits- und Urlaubsdaten auf den Festplatten vorhanden waren.
Zudem konnte man aus noch vorhandenen Browsercaches u. a. die Hobbies/Interessen des jeweiligen Mitarbeiters sowie dessen dienstliches Aufgabengebiet einschätzen.
Der TLfDI bat daraufhin die Kraftwerke Gera GmbH unter anderem um die Übersendung des datenschutzrechtlichen Sicherheitskonzepts und der Dienstanweisungen, aus denen sich ergibt, inwieweit Mitarbeiter/-innen der Kraftwerke Gera GmbH vor Aussonderung ihrer Dienst-PCs angehalten sind, personenbezogene Daten auf den Dienst-PCs zu löschen.
Die Kraftwerke Gera GmbH teilte mit, dass sie nicht über eigenes IT-Personal verfüge, sondern in den Konzernverband der Stadtwerke Gera AG eingebunden sei, wobei die Stadtwerke mit der IT-

Betreuung und der Entsorgung jeglicher Hardware beauftragt worden seien. Zudem verwies die Kraftwerke Gera GmbH auf Geschäftsanweisungen zum Umgang mit Daten, in denen auch die Löschung und Vernichtung von Daten vorgesehen sei.
Im Rahmen der weiteren Prüfung informierte die Kraftwerke Gera GmbH den TLfDI, dass es ihr gelungen sei, betriebsintern aufzuklären, wer für den Vorfall der datenschutzwidrigen Entsorgung der Festplatten auf dem Werkstoffhof verantwortlich sei. Es handelte sich dabei um einen Mitarbeiter der Kraftwerke Gera GmbH, der beide Festplatten widerrechtlich und wissentlich mit nach Hause genommen, sie dort weitergenutzt und anschließend nach längerer Lagerung über den Elektroschrott entsorgt hatte. Die Kraftwerke Gera GmbH fügte quasi als Beweis für die Glaubhaftigkeit dieses Sachverhalts auch ein Schreiben an, in dem der Mitarbeiter seine Verfehlungen einräumte.
Unabhängig davon steht aus datenschutzrechtlicher Sicht fest, dass die Kraftwerke Gera GmbH als verantwortliche Stelle gemäß § 9 BDSG die technischen und organisatorischen Maßnahmen zu treffen hat, die erforderlich sind, um die Ausführung datenschutzrechtlicher Bestimmungen zu gewährleisten. Dies ergibt sich aus § 2 Abs. 2 ThürDSG, da es sich bei der Kraftwerke Gera GmbH um eine öffentliche Stelle handelt, die am wirtschaftlichen Wettbewerb teilnimmt und auf die nach § 26 ThürDSG nur die Bestimmungen des 5. Abschnitts des ThürDSG (ausgenommen § 34 Abs. 2 ThürDSG) anzuwenden sind. Im Übrigen gelten für sie die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mit Ausnahme des 2. Abschnitts und des § 38 BDSG.
Die von der Kraftwerke Gera GmbH getroffenen technischen und organisatorischen Maßnahmen waren deshalb verbesserungsbedürftig, um künftig solche Fallkonstellationen wie hier geschildert zu verhindern, bzw. weitestgehend auszuschließen. Da die Kraftwerke Gera GmbH aber selbst nicht nur tatkräftig an der lückenlosen Aufklärung dieses Falles mitwirkte, sondern konstruktiv auch die entsprechenden datenschutzrechtlichen Lehren aus diesem Fall zog, sagte sie zu, ihr Sicherheitskonzept dergestalt zu verbessern, dass konkrete Handlungsanweisungen für den sicheren Umgang (insbesondere die Löschung und die Vernichtung) von personenbezogenen Daten aufgenommen werden sollten. Diese und weitere Verbesserungen in ihren technischen und organisatorischen Maßnahmen hat

die Kraftwerke Gera GmbH nunmehr dem TLfDI zur abschließenden Prüfung vorgelegt.

Die verantwortliche Stelle hat gemäß § 9 BDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung datenschutzrechtlicher Bestimmungen zu gewährleisten. Dazu zählt es auch, Regelungen zu treffen, aus denen klar hervorgeht, durch wen und durch welche geeigneten Maßnahmen Festplatten und andere elektronische Speichermedien datenschutzkonform zu vernichten sind.

Personal Personalakte – © Wolfilser / Fotolia.com

6 Personaldaten

6.1 Datenleck bei Betriebsratswahl

In einem Eigenbetrieb eines Landkreises hatten Betriebsratswahlen stattgefunden. Die Unterlagen hierzu wurden im Auftrag des Wahlvorstands unter Verschluss genommen und versiegelt und unter Versicherung, dass keine Kopien hiervon existierten, dem neuen Betriebsrat entsprechend der Vorschriften des Betriebsverfassungsgesetzes übergeben. Zum öffentlichen Kammertermin zur Wahlanfechtung vor dem Arbeitsgericht staunte der neue Betriebsrat, der den versiegelten Packen Unterlagen dabei hatte, allerdings darüber, dass das Gericht und alle Arbeitgebervertreter mit Kopien eben dieser Wahlunterlagen ausgestattet waren. Da diese Unterlagen personenbezogene Daten enthielten, wandte sich der Betriebsrat und Wahlvorstand an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem er bereits Strafantrag wegen der Veröffentlichung vertraulicher Unterlagen gestellt hatte.
Die Wahl war letztendlich vom Gericht als nichtig erklärt worden, wobei man festgestellt hatte, dass ein Mitglied des Wahlvorstands

regelwidrig Wahlvorschläge entgegengenommen und kurzerhand für unzulässig erklärt hatte.
Der TLfDI konnte wegen der Dringlichkeit der Angelegenheit zunächst nur eine vorläufige Einschätzung vornehmen. Wahlunterlagen enthalten personenbezogen Daten und dienen dazu, den Nachweis der ordnungsgemäßen Durchführung zu erbringen. Zum Zweck der Wahlanfechtung kann Einblick genommen werden. Auch Unterstützungsunterschriften können zum Zweck der Einschätzung der Wirksamkeit überprüft werden, selbst wenn der Wahlvorstand ursprünglich irrtümlich gegenüber den unterzeichneten Unterstützern die Versicherung abgegeben hatte, dass die Unternehmensleitung davon nichts erfahre.
Der Betriebsrat bat den TLfDI, datenschutzrechtliche Maßnahmen einzuleiten. Der Eigenbetrieb war privatrechtlich organisiert, unterlag jedoch aufgrund der Beteiligung des Landkreises dem Thüringer Datenschutzgesetz (ThürDSG), § 1 Abs. 2 Satz 1 ThürDSG. Ein Betriebsrat ist der Stelle zuzuordnen, auch wenn er die gesonderte Aufgabe hat, die Beschäftigteninteressen gegenüber der Unternehmensleitung zu vertreten. Nach der Aufgabenwahrnehmung des Eigenbetriebs war er als Wettbewerbsunternehmen einzuordnen, sodass nach § 26 ThürDSG nur der Fünfte Abschnitt des ThürDSG anzuwenden war, im Übrigen die Bestimmungen des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts und des § 38. Daher war zu prüfen, ob ein Ordnungswidrigkeitenverfahren gegen ein Mitglied des Wahlvorstands eingeleitet werden konnte, das nach Auffassung der Beschwerdeführer der Unternehmensleitung bewusst die Unterlagen unzulässigerweise zugespielt hatte. Da aber bereits ein entsprechender Strafantrag bei der zuständigen Staatsanwaltschaft gestellt war, ist zunächst der Ausgang des Strafverfahrens abzuwarten. Unter Umständen kann danach ein Ordnungswidrigkeitsverfahren eingeleitet werden, wenn ersteres Verfahren eingestellt werden sollte.

Unterlagen mit personenbezogenen Daten sind gegen unbefugte Kenntnis zu schützen. Die besten technischen und organisatorischen Maßnahmen gehen ins Leere, wenn eine befugte Person die Unterlagen bewusst pflichtwidrig anderen Personen zugänglich macht. Das unbefugte Zugänglichmachen kann als Straftat oder Ordnungswidrigkeit geahndet werden. Die Einleitung eines Ordnungswidrigkei-

tenverfahrens durch den TLfDI entfällt, wenn bereits ein Strafverfahren eingeleitet wurde.

6.2 Darf der behördeninterne Datenschutzbeauftragte den Personalrat kontrollieren?

Ein Mitglied eines Personalrats bei einer Thüringer Behörde wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob der behördliche Datenschutzbeauftragte der Dienststelle denn befugt sei, den Personalrat zu überprüfen. Die geschilderte Situation gestaltete sich so, dass der Personalrat keinen eigenen Raum für die Personalratsarbeit zur Verfügung hatte. Den Vorsitzenden und den Stellvertreter hatte man einfach in einem Büroraum untergebracht, wo jeder zur Hälfte seiner jeweiligen Arbeitszeit sowohl Personalratsarbeit als auch behördliche Verwaltungstätigkeit verrichten sollte. Ein verschließbarer Schrank stand zur Verfügung, in dem die Unterlagen, die zur Personalratsarbeit benötigt werden, eingeschlossen werden konnten, um unbefugte Kenntnis während der „normalen Dienstzeiten“ mit Publikumsverkehr zu verhindern. Auch erhielt der Personalrat eine Sekretärin, die mit einem nicht unwesentlichen Teil ihrer Arbeitszeit, aber auch einem Fachdienst- und Amtsleiter zur Verfügung zu stehen hatte. Die Arbeit für den Personalrat erledigte sie auf einem Notebook, das sie zum Schutz vor unbefugter Einsicht jeweils zuklappen konnte, wenn ihr jemand über die Schulter schauen konnte oder wollte.
Datenschutzrechtlich ist der Personalrat einer Dienststelle als Teil dieser Dienststelle zu bewerten. Die Pflicht zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften trifft jedoch die verantwortliche Stelle nach § 34 Thüringer Datenschutzgesetz (ThürDSG), also die Dienststelle. Auch beim Personalrat müssen die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten, die im Rahmen seiner Aufgabenerfüllung verarbeitet werden, getroffen sein. Werden Mängel festgestellt, ist die Dienststelle aufgerufen, geeignete Maßnahmen zu treffen, damit die Mängel behoben werden. Hierfür sind dem Personalrat von der Dienststelle auch die Mittel zur Verfügung zu stellen, damit die datenschutzrechtlichen Vorschriften eingehalten werden können.

Unter den in der betroffenen Dienststelle herrschenden Umständen fällt es nicht leicht, die an den Personalrat von den Beschäftigten herangetragenen Anliegen vertraulich zu behandeln und die erforderlichen Maßnahmen zum Schutz personenbezogener Daten der Beschäftigten (oftmals Personalaktendaten), die im Rahmen der Mitbestimmung dem Personalrat von der Dienststelle übermittelt werden müssen, einzuhalten.
Nun hatte der Dienststellenleiter den behördlichen Datenschutzbeauftragten (bDSB) mit einer datenschutzrechtlichen Überprüfung des Personalrats beauftragt und der Personalrat vermutete dahinter keine guten Absichten. Etwas Würze bekam die Sache dadurch, weil es sich beim behördlichen Datenschutzbeauftragten um den ehemaligen Personalratsvorsitzenden handelte, der möglicherweise Freude oder Genugtuung über aufgespürte Fehler seiner Nachfolger haben könnte.
Hierzu hat der TLfDI Folgendes ausgeführt: Die Zuständigkeit und die Befugnisse des Beauftragten für den Datenschutz sind in § 10a ThürDSG festgelegt. Zwar hat das Bundesarbeitsgericht (BAG) in seinem Beschluss vom 11. November 1997 entschieden, dass eine Kontrollbefugnis des betrieblichen Datenschutzbeauftragten für Betriebsräte nicht besteht. Gleichzeitig hat es allerdings dargelegt, dass das Bundesverwaltungsgericht die Frage der Kontrollbefugnis des betrieblichen Datenschutzbeauftragten in Bezug auf die Personalverwaltung im öffentlichen Dienst ausdrücklich offen gelassen hat (BAG, Beschluss vom 11. November 1997, Az.: 1 ABR 21/97, Rn. 31).
Nach § 10a Abs. 2 ThürDSG hat der Beauftragte für den Datenschutz die Aufgabe, die Daten verarbeitende Stelle bei den Ausführungen der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. Dies gilt grundsätzlich auch für den Personalrat, der als Teil der Dienststelle, die für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist, hiervon nicht grundsätzlich ausgenommen ist. Auch das Thüringer Personalvertretungsgesetz enthält keine Ausnahmeregelung. Eine Ausnahme besteht aber im Hinblick auf personenbezogene Daten in oder aus Personalakten, die nur mit Einwilligung der Betroffenen durch den Beauftragten für den Datenschutz einsehbar sind (§ 10a Abs. 4 Satz 1 ThürDSG). Zudem besteht ein besonderes Amtsgeheimnis der Personalratsmitglieder hinsichtlich der personenbezogenen Daten, die ihnen in ihrer Aufgabenwahrnehmung

bekannt geworden sind. Soweit also Personalaktendaten und einem besonderen Amtsgeheimnis unterliegende personenbezogene Daten beim Personalrat vorhanden sind, dürfen diese vom Beauftragten für den Datenschutz in seiner Aufgabenwahrnehmung nicht ohne Einwilligung des einzelnen Betroffenen eingesehen werden.
Im Falle einer Prüfung durch den behördlichen Datenschutzbeauftragten ist darüber hinaus auch die Sensibilität der Personalratstätigkeit zu beachten. Mitarbeiter dürfen sich vertrauensvoll an den Personalrat wenden, ohne dass die Dienststellenleitung davon über eine Kontrolle des Datenschutzbeauftragten Kenntnis erhalten könnte. Andererseits kann eine Prüfung durch den behördlichen Datenschutzbeauftragten in partnerschaftlicher Zusammenarbeit mit dem Personalrat auch Missstände, wie sie im vorliegenden Fall vorlagen, z. B. die ungeeigneten Räumlichkeiten, Mängel bei der Möglichkeit für Mitarbeiter, sich ungehindert an den Personalrat wenden zu können, ohne dass dies anderen Personen als den berechtigten Personalratsmitgliedern zur Kenntnis gelangt, aufzeigen und dazu beitragen, datenschutzgerechte Lösungen zu finden.
Der TLfDI beschränkte sich bis jetzt auf beratende Unterstützung, behält sich aber eine Kontrolle vor Ort vor.

Eine Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Personalrat durch den behördlichen Datenschutzbeauftragten ist nicht vollständig ausgeschlossen. Im Falle einer Prüfung dürfen jedoch vom behördlichen Datenschutzbeauftragten grundsätzlich keine personenbezogenen Daten der Beschäftigten zur Kenntnis genommen werden, die dem Personalrat zur Aufgabenerfüllung vorliegen. Die datenschutzrechtliche Prüfung hat sich daher auf das Vorliegen geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten zu beschränken. Die Dienststelle hat dem Personalrat die erforderlichen Mittel zur Verfügung zu stellen, damit durch den Personalrat selbst geeignete Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften getroffen werden können.

6.3 Zeitungsnotiz zur „krankheitsbedingten“ Schließung eines Amtes

Eine Stadtverwaltung aus dem Saaleholzlandkreis (SHK) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Bewertung folgenden Sachverhalts:
Die Stadtverwaltung hatte in der Regionalzeitung über eine „krankheitsbedingte“ Schließung ihres Ordnungsamtes informiert.
Die Sorge und Frage der Stadt an den TLfDI war nun, ob aufgrund einer solchen Zeitungsnotiz außenstehende Dritte mit einer gewissen Wahrscheinlichkeit auf die Krankheit einer bestimmten Mitarbeiterin der Stadtverwaltung schließen könnten.
Diese Frage konnte der TLfDI nicht „pauschal“ beantworten. Vielmehr kommt es auf die Umstände des Einzelfalls an. Insbesondere spielen die Anzahl der Mitarbeiter des betreffenden Amtes sowie die Bekanntheit des Amtsleiters bei den Bürgern eine Rolle, die naturgemäß in einer Kleinstadt höher sein wird als in einer Großstadt mit einer eher anonym agierenden Verwaltung.
In dieser Stadtverwaltung bestand das Ordnungsamt aus zwei Mitarbeiterinnen. Insofern entspricht es der Lebenserfahrung, dass Dritte unter Berücksichtigung der für eine Kleinstadt typischen Zusatzinformationen, wie z. B. Mitteilungen von gemeinsamen Bekannten und zufällige Beobachtungen der Betroffenen innerhalb ihrer sonstigen Arbeitszeit bei nicht-dienstlichen Tätigkeiten, mit einer relativ hohen Wahrscheinlichkeit auf eine Krankheit der Betroffenen schließen könnten.
Aufgrund der Mitarbeiterzahl im Ordnungsamt im konkreten Fall handelte es sich bei der betreffenden Veröffentlichung – der „krankheitsbedingten“ Schließung – um eine unerlaubte Übermittlung einer Einzelangabe zu einer bestimmbaren Person im Sinne des § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) an Stellen außerhalb des öffentlichen Bereichs (§ 22 ThürDSG). Vorstellbar wäre eine solche Veröffentlichung ggf. nur dann, wenn die Betroffene darin eingewilligt hat. Selbstverständlich bezieht sich die o. g. Bewertung auch auf die Übermittlung solcher personenbezogenen bzw. -beziehbaren Daten zu erkrankten Mitarbeitern der Stadtverwaltung innerhalb öffentlicher Sitzungen des Stadtrates und auf Informationen der Stadtverwaltung gegenüber Bürgern mittels Internet und E-Mail.

Nachfolgend bat der TLfDI die Stadtverwaltung aufgrund seiner Bewertung des Sachverhalts darum, den Vorfall auszuwerten und künftig in ähnlichen Fällen datenschutzrechtskonform zu handeln. Daraufhin teilte die Stadtverwaltung mit, dass eine Dienstanweisung in Vorbereitung sei, wonach künftig nur noch das Datum und der (voraussichtliche) Zeitraum der Abwesenheit ohne Nennung des Grundes der Abwesenheit mitgeteilt werde. Ferner sagte die Stadtverwaltung zu, künftig bei der Veröffentlichung in Zeitungen oder in Amtsblättern Formulierungen zu verwenden, die einen Rückschluss auf eine bestimmte oder bestimmbare Person ausschließen.

Öffentliche Stellen haben bei Veröffentlichungen in Zeitungen oder in Amtsblättern dafür Sorge zu tragen, zu verhindern, dass Außenstehende aus einer Information, wie z. B. der „krankheitsbedingten" Schließung eines Amtes, auf eine bestimmte Person schließen können. Wegen der Unzulässigkeit einer solchen Übermittlung personenbezogener bzw. -beziehbarer Daten sollte die öffentliche Stelle im Zweifelsfall ganz auf die Angabe eines bestimmten Grundes verzichten. Dies gilt umso mehr, je weniger Personal die öffentliche Stelle bzw. ihre Organisationseinheit besitzt.

6.4 Mitarbeiter: Bitte lächeln!

Der Beauftragte für den Datenschutz einer Thüringer Kommune bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung zu dem Vorhaben, Bilder von Beschäftigten in eigenen Prospekten, Flyern oder der Tageszeitung zu veröffentlichen. Ohne weitere Hintergrundinformationen, beispielsweise zu welchem Zweck welche konkreten Bilder von Beschäftigten veröffentlicht werden sollen, hat der TLfDI im Rahmen seiner Beratungsaufgabe nach § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hierzu allgemein ausgeführt:
Fotografien von Mitarbeitern der Stadtverwaltung sind personenbezogene Daten von Beschäftigten, die gemäß § 33 Abs. 1 ThürDSG nach den dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) verarbeitet werden dürfen. Bei der Verwendung von Fotografien von Mitarbeitern handelt es sich regelmäßig nicht um eine Aufgabe der Personalverwaltung und -bewirtschaftung, sodass dies nur mit Einwilligung der Betroffenen geschehen kann. Es muss jedoch zur Einholung einer Einwilligung

vorab geprüft werden, dass eine Erforderlichkeit zur Aufgabenerfüllung vorliegt. Eine öffentliche Stelle wie die Stadtverwaltung muss daher auch bei der Veröffentlichung von Mitarbeiterbildern an die Erforderlichkeit zur Aufgabenerfüllung anknüpfen.
Handelt es sich um Bilder des Bürgermeisters oder der Beigeordneten, die in Wahrnehmung von öffentlichen Veranstaltungen und Terminen entstanden sind, bedarf es aufgrund deren Stellung sozusagen als Personen der Zeitgeschichte keiner Einwilligung zur Veröffentlichung von Bildern.
Die Einwilligungserklärung zum Abdruck in Druckerzeugnissen (stadteigenen Prospekten und Flyern) ist an die formellen Voraussetzungen des § 4 Abs. 3 ThürDSG gebunden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Beschäftigten müssen auf den Zweck und den Umfang der beabsichtigten Veröffentlichung hingewiesen werden. Weiterhin muss die Einwilligung auf Freiwilligkeit beruhen. Sollte die Stadtverwaltung Aufnahmen von Mitarbeitern an die Tageszeitung zur Veröffentlichung geben, gilt dies ebenso. Sofern daran gedacht wird, dass die Prospekte und Flyer auch im Internet Veröffentlichung finden, ist § 23 ThürDSG zu beachten. Bei der Veröffentlichung von Daten im Internet handelt es sich um eine Übermittlung personenbezogener Daten an öffentliche und nichtöffentliche Stellen außerhalb des Geltungsbereiches des Grundgesetzes. Eine solche Übermittlung ist nur unter den Voraussetzungen des §°23 ThürDSG zulässig. Da nicht ausgeschlossen werden kann, dass bei einer weltweiten Veröffentlichung die Daten auch in Staaten übermittelt werden, in denen kein angemessenes Datenschutzniveau gewährleistet ist, müssen die Voraussetzungen des § 23 Abs. 2 ThürDSG gegeben sein. Von diesen Voraussetzungen kommt allenfalls die Nr. 1 in Betracht, nach der eine zweifelsfreie Einwilligung des Betroffenen vorliegen muss.
Die Einwilligung ist nach § 4 Abs. 2 ThürDSG die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seinen personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen. Sofern der Betroffene, dessen Daten veröffentlicht werden, in einem Arbeitsverhältnis mit der Daten übermittelnden Stelle steht, bestehen bereits große Zweifel an der Freiwilligkeit der Einwilligung. Freiwilligkeit ist nur dann gegeben, wenn für die Mitarbeiter keinerlei Druck besteht und im Falle einer Ablehnung auch keine Nachteile entstehen. Diesen Grundsatz

hat auch das Bundesarbeitsgericht insbesondere zur Einwilligung im Sinne des § 22 Kunsturhebergesetz in jüngster Zeit ausgeführt (Vgl. BAG Urteil vom 19. Februar 2015 – 8 AZR 1011/13). Die Einwilligung kann jederzeit zurückgenommen werden. Wird die Einwilligung zurückgenommen, muss die Datenübermittlung für die Zukunft unterbleiben. In diesem Fall ist auch die Speicherung des Fotos auf dem Server unzulässig und der Betroffene hat einen Anspruch auf Löschung nach § 16 Abs. 1 Nr. 1 ThürDSG.

Grundsätzlich ist es nicht Aufgabe einer öffentlichen Stelle, Mitarbeiterfotos zu veröffentlichen. Eine Veröffentlichung ohne besonderen Darstellungsgrund ist daher unzulässig. Sollen Beschäftigtenfotos durch öffentliche Stellen auf der Grundlage des Kunsturhebergesetzes veröffentlicht werden, sind hierzu zweifelsfrei freiwilllige Einwilligungen der Betroffenen erforderlich. Den Beschäftigten darf insbesondere bei Verweigerung der Einwilligung keinerlei Nachteil entstehen.

6.5 Bewerberunterlagen: Einsicht für alle Personalratsmitglieder?

Der Personalratsvorsitzende in einem Landratsamt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob denn nur der Personalratsvorsitzende oder auch andere Personalratsmitglieder Einsicht in Bewerberunterlagen nehmen dürften. Hintergrund war folgender:
Dem Personalrat steht bei Einstellungen gemäß § 68 Abs. 2 Satz 4 Thüringer Personalvertretungsgesetz (ThürPersVG) das Recht zur Einsichtnahme in die Bewerbungsunterlagen aller Mitbewerber zu, um Benachteiligungen jeglicher Art auszuschließen. Dementsprechend ist die Dienststelle zur Vorlage der Bewerbungsunterlagen an den Personalrat verpflichtet. Die Dienststelle wollte das Einsichtsrecht mit Hinweis auf den besonderen Schutz von Bewerberdaten auf den Personalratsvorsitzenden beschränken.
Im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern wurde aber die Zuständigkeit der einzelnen Mitglieder auf verschiedene Ämter aufgegliedert. Das jeweils zuständige Mitglied nimmt folglich auch an den Bewerbergesprächen teil. Wenn die Einsicht in die entsprechenden Bewerberunterlagen auf den Personalratsvorsitzenden beschränkt bliebe, wäre das für das entsprechen-

de Bewerbungsverfahren zuständige Personalratsmitglied auf die Weitergabe der entsprechenden Informationen vom Vorsitzenden angewiesen.
Zur Beantwortung der Frage führte der TLfDI aus, dass aus den datenschutzrechtlichen Grundsätzen die Dienststellenleitung verpflichtet ist, nur die für eine Personalmaßnahme erforderlichen personenbezogenen Daten dem Personalrat zugänglich zu machen. Bei der Einstellung eines Bewerbers sind die Unterlagen des Bewerbers sowie seiner Mitbewerber für die Entscheidung des Personalrats erforderlich. Auch wenn Bewerberdaten eine besondere Sensibilität zukommt, muss dem Personalrat zur Gewährleistung seiner Handlungsfähigkeit Kenntnis der erforderlichen Daten gewährt werden. Aufgrund der Sensibilität der personenbezogenen Daten der Bewerber ist es hingegen nicht erforderlich, dem gesamten Personalrat, also allen seinen Mitgliedern, den Zugang zu den personenbezogenen Daten zu gewähren. Wird jedoch, wie vorliegend geschildert, im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern die Zuständigkeit der einzelnen Personalratsmitglieder auf verschiedene Ämter aufgegliedert, müssen für das jeweils zuständige Personalratsmitglied, das an den Bewerbungsgesprächen teilnimmt, auch die für die Aufgabenwahrnehmung erforderlichen personenbezogenen Daten der Bewerber zugänglich sein.
Aus datenschutzrechtlicher Sicht sah der TLfDI daher keine Gründe, diesem zuständigen Personalratsmitglied die Einsicht in die zu seiner Aufgabe erforderlichen entsprechenden Bewerbungsunterlagen zu verweigern und diese nur dem Personalratsvorsitzenden zu gewähren, der das Mitglied entsprechend informieren müsste. Soweit aber dem zuständigen Personalratsmitglied die Daten zugänglich gemacht werden, ist darüber hinaus eine Vorlage an den Personalratsvorsitzenden oder andere Mitglieder des Personalrats grundsätzlich nicht mehr erforderlich.

Dem Personalrat müssen die zu seiner Aufgabenerfüllung erforderlichen Bewerberdaten von der Dienststelle zugänglich gemacht werden. Die Einsicht ist in die Unterlagen zu gewähren, soweit sie für die Aufgabenerfüllung des Personalrats erforderlich ist. Hat der Personalrat einzelne Aufgaben auf einzelne Personalratsmitglieder delegiert, reicht es aus, nur diesen Zugang zu den zur Aufgabenerfüllung erforderlichen personenbezogenen Daten von Bewerbern zu gewähren.

6.6 „Pranger 2.0“ – Amtsleiter stellt sensible Daten von Mitarbeiterin ins Intranet

Eine Mitarbeiterin einer Stadtverwaltung teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Folgendes mit: Der Leiter eines städtischen Amtes habe ein Schreiben des Haupt- und Personalamtes mit sensiblen Daten zu ihrer Person aus einem Verfahren zur Vermeidung und Bekämpfung von Mobbing anderen Mitarbeitern der Stadtverwaltung über das Intranet zur Kenntnis gegeben. Eine Einwilligung der Mitarbeiterin der Stadtverwaltung zu dieser Datenübermittlung lag natürlich nicht vor.
Der TLfDI stellte schnell fest, dass die interne Veröffentlichung sensibler personenbezogener Daten aus einem Verfahren zur Dienstvereinbarung Mobbing an nicht am Verfahren beteiligte Personen im konkreten Fall unzulässig erfolgte und dies einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften darstellte. Daher hat der TLfDI die datenschutzrechtlichen Mängel in Form einer nach § 21 Thüringer Datenschutzgesetz (ThürDSG) unzulässigen Übermittlung personenbezogener Daten gemäß § 39 Abs. 1 Satz 1 ThürDSG beanstandet. Der TLfDI forderte die Stadtverwaltung auf, dafür Sorge zu tragen, dass künftig in ähnlichen Fällen die Datenübermittlung auf den Kreis der Berechtigten beschränkt wird. Die betroffene Stadtverwaltung hat zu der Angelegenheit ein Ordnungswidrigkeitenverfahren eingeleitet.

Wenn ein Amtsleiter einer Thüringer Stadtverwaltung hochsensible Daten aus einem Mobbing-Bekämpfungsverfahren nicht am Verfahren Beteiligten zur Kenntnis gibt, zeugt dies von einer Unkenntnis bzw. Ignoranz über Grundprinzipien des Datenschutzes und zeigt den nach wie vor bestehenden immensen Informationsbedarf in Sachen Datenschutz. Der TLfDI wird sich dieser dringlichen Aufgabe weiterhin stellen und deshalb sowohl die Kommunen beraten als auch Gemeinden und Landkreise kontrollieren.

6.7 Mitarbeiter im GPS-Dauer-Fokus

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass in Fahrzeugen

eines Zweckverbands zur Wasser- und Abwasserversorgung GPS-Technik eingesetzt werde. Diese Technik ist dazu geeignet, jederzeit den Standort eines Fahrzeugs festzustellen und eine Leistungs- und Verhaltenskontrolle der Mitarbeiter durchzuführen. Der Zweck des GPS-Einsatzes in den Fahrzeugen war nicht bekannt, da sich die Mitarbeiter nicht ausreichend informiert sahen. Festlegungen zum Umgang mit mittels GPS erhobenen personenbezogenen Daten der Kraftfahrzeugnutzer sowie Regelungen zum Zugriff und zur Nutzung der Fahrzeuge gab es nicht.

Auf Anfrage des TLfDI gab der Zweckverband an, dass die Fahrzeuge tatsächlich mit GPS-Geräten ausgestattet seien, um den Standort dieser Fahrzeuge schnell lokalisieren zu können. Dies sei für die Koordinierung der täglichen Einsätze insbesondere im Havariefall vorteilhaft, um Ausfallzeiten in der Wasserversorgung zu minimieren. Einen positiven Nebeneffekt sah man darin, dass die Fahrzeuge im Falle des Diebstahls wieder aufgefunden werden könnten, zumal in den letzten Jahren bereits Fahrzeuge gestohlen worden waren.

Die durch GPS übermittelten Daten zu den Fahrzeugen wurden auf einem externen Server für 90 Tage vorgehalten. Dort ist eine Zusammenführung mit den Fahrerdaten nicht möglich. Die Mitarbeiter seien über die Gründe und den Einsatz der Geräte mündlich informiert worden. Schriftliche detaillierte Informationen sollten jedoch erst nach Abschluss einer Testphase erfolgen bzw. wurden zum damaligen Zeitpunkt erarbeitet. Zur eingehenden datenschutzrechtlichen Prüfung waren diese Angaben selbstverständlich nicht ausreichend.

Durch GPS erhobene Standortdaten oder Bewegungsprofile von Fahrzeugen sind personenbeziehbare und damit personenbezogene Daten, wenn sie einem konkreten Fahrer zugeordnet worden sind. Damit verbunden ist, dass der jeweilige Beschäftigte einer Leistungs- und Verhaltenskontrolle unterzogen werden kann, die nach § 33 Abs. 4 Thüringer Datenschutzgesetz (ThürDSG) unzulässig ist.

Nach § 19 Abs. 2 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Zu dem angegebenen Zweck der Standortlokalisierung zur Koordinierung der täglichen Einsätze ist eine Erforderlichkeit zur Erfassung der Position während der Fahrt gegeben. Eine Erforderlichkeit zur Erfassung z. B. der gefahrenen Geschwindigkeit ist nicht ersichtlich und damit unzulässig.

Nach § 20 Abs. 1 ThürDSG ist die Speicherung der Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Zur Feststellung der Position für Einsatzzwecke ist eine aktuelle Positionsbestimmung ausreichend. Hierfür bedarf es keiner über das Tagesende hinaus andauernden Speicherung. Aus der Feststellung der Fahrzeugposition im Fall eines Diebstahls ist eine Echtzeitfeststellung ausreichend. Die Speicherung der Fahrzeugdaten für 90 Tage war daher nicht begründbar und mangels Erforderlichkeit unzulässig. Der TLfDI forderte daher, dass mangels Rechtsgrundlage die Geschwindigkeitserfassung zu deaktivieren ist und die gespeicherten Daten zu löschen sind.
Die im Nachgang erarbeitete Dienstanweisung enthält nunmehr eine Auflistung der erfassten Daten, konkrete Festlegungen zur Zweckbindung und der Zugriffs- und Nutzungsrechte. Die Nutzung der erfassten Fahrzeugdaten zur Verhaltens- und Leistungskontrolle der Fahrzeugführer ist ausgeschlossen. Die Dauer der Speicherung wurde auf 72 Stunden verkürzt. Diese Speicherungsdauer kann ausnahmsweise damit begründet werden, dass unter Umständen ein zulässiger Zugriff am Montag auf den vorhergehenden Freitag erforderlich sein kann.

Wird in Fahrzeugen GPS eingesetzt, bedarf es konkreter Festlegungen in einer Dienstvereinbarung beziehungsweise einer Dienstanweisung. In dieser sind der konkrete Zweck der Fahrzeugdatenerfassung, die zu erfassenden Daten sowie die Dauer der Speicherung festzulegen und es ist zu bestimmen, zu welchem Zweck die Daten ausgewertet werden dürfen. Eine Verhaltens- und Leistungskontrolle der Fahrzeugführer ist auszuschließen (§ 33 Abs. 4 ThürDSG).

6.8 Übermittlungsbefugnis des Amtsarztes – keine Generalvollmacht!

Auch in diesem Berichtszeitraum zeigte sich, dass der Umfang der Offenbarungsbefugnis des Amtsarztes gegenüber der anfordernden Behörde nicht immer eingehalten wird (vgl. zuletzt 9. TB Punkt 6.2). Der Umfang der Offenbarungsbefugnis des mit der Untersuchung beauftragten Amtsarztes gegenüber der anfordernden Behörde wurde neu geregelt. Sie richtet sich seit 1. Januar 2015 nach § 33 Abs. 3

und 4 Thüringer Beamtengesetz (ThürBG). Danach teilt der Arzt der zuständigen Behörde die tragenden Feststellungen und Gründe des Ergebnisses der ärztlichen Untersuchung mit, soweit deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist. Ferner berichtet er über die infrage kommenden Maßnahmen zur Wiederherstellung der Dienstfähigkeit und die Möglichkeit einer anderen Verwendung. Als technische und organisatorische Maßnahmen zum Schutz dieser sensiblen Angaben ist weiterhin gesetzlich bestimmt, dass die Mitteilung des Arztes über die Untersuchungsergebnisse in einem gesonderten, verschlossenen und versiegelten Umschlag zu übersenden ist. Sie ist verschlossen zur Personalakte des Beamten zu nehmen. Weiterhin dürfen die an die Behörde übermittelten Daten nur für die im Einzelfall konkret zu treffende Entscheidung verarbeitet oder genutzt werden. Somit ist auch eine besondere Zweckbindung festgeschrieben.
Die Transparenz für die Betroffenen wurde ebenfalls berücksichtigt. Nach § 33 Abs. 2 ThürBG ist der Beamte zu Beginn der Untersuchung oder der Beobachtung auf deren Zweck und die Übermittlungsbefugnis an die Behörde hinzuweisen. Der Arzt übermittelt dem Beamten oder, soweit dem ärztliche Gründe entgegenstehen, dessen Bevollmächtigten eine Kopie der an die Behörde erteilten Auskünfte.
Eine in diesem Sinne betroffene Person wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem sie vom Amtsarzt keine Auskunft dazu erhielt, was denn nun an die personalverwaltende Dienststelle als Ergebnis einer Untersuchung gesandt worden war. Nachdem sie sich an ihre Personalverwaltung gewandt und Einsicht in die Unterlagen genommen hatte, fiel sie aus allen Wolken. Es waren alle erdenklichen Diagnosen aufgeführt, ob sie nun mit der Dienstfähigkeit in Verbindung standen oder nicht. Weiterhin machte die betroffene Person geltend, sie habe eine Schweigepflichtentbindungserklärung in pauschaler Form vorgelegt erhalten, die sie bereits vor der Untersuchung unterschreiben sollte, obwohl weder die zu entbindenden Ärzte noch der konkrete Zweck darin erkennbar waren.
Nachdem der TLfDI gegenüber dem Amtsarzt die Rechtslage dargelegt hatte, sagte dieser unverzüglich zu, zukünftig nur noch die für die Kenntnis der Behörde für die von ihr zu treffende Entscheidung erforderlichen Angaben zu übermitteln. Weiterhin werde zukünftig

beachtet, dass auch die begutachteten Beamten einen Anspruch auf eine Kopie der an die Behörde erteilten Auskünfte haben. Die formularmäßige Entbindung von der Schweigepflicht für behandelnde andere Ärzte wurde überarbeitet und konkretisiert, sodass zukünftig wirksame Schweigepflichtentbindungen erteilt werden können.
Aufgrund der prompten Zusage zur Behebung der erheblichen datenschutzrechtlichen Verstöße hat der TLfDI unter Anwendung des § 39 Abs. 3 ThürDSG zunächst von einer Beanstandung nach § 39 Abs. 1 ThürDSG abgesehen. Nachdem sich aber die Beschwerdeführerin nach Ablauf einer angemessenen Frist wieder meldete, weil sie auf ihre Anfragen und Bemühungen immer noch keine Kopie des „neuen", den gesetzlichen Anforderungen entsprechenden Gutachtens erhalten habe, musste der TLfDI davon ausgehen, dass die Zusagen (noch) nicht umgesetzt wurden. Daher sprach er eine Beanstandung nach § 39 Abs. ThürDSG in Verbindung mit § 33 Abs. 3 und 5 ThürBG mit Fristsetzung zur Behebung der datenschutzrechtlichen Mängel aus.

Es ist zu erwarten, dass den Amtsärzten in Wahrnehmung ihrer Aufgabe die gesetzlichen Vorschriften geläufig sind und damit die Übermittlung von Angaben bzw. Diagnosen unterbleibt, die nicht für die Entscheidung der Auftrag gebenden Behörde erforderlich sind.

6.9 GPS: nicht vom richtigen Weg abkommen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Information, dass die Stadtwerke Schmölln GmbH ihre Fahrzeuge mit Möglichkeiten zu einer **G**lobal **P**ositioning **S**ystem (kurz GPS)-Überwachung und damit zu einer weitgehenden Verhaltens- und Leistungskontrolle der jeweiligen Fahrer ausgestattet hätten.
Der TLfDI nahm sich dieses Falles an und forderte die Stadtwerke zu einer Stellungnahme auf. Aus dieser ging hervor, dass eine Auswertung des GPS-Systems zu Kontrollzwecken erfolge, wenn der Verdacht bestehe, dass Fahrzeuge zu betriebsfremden, nicht genehmigten Fahrten benutzt werden oder wenn der Verdacht einer Straftat vorliege. Eine Rechtsgrundlage für die Überprüfung der Protokolldaten (u.a. die Fahrzeit und Fahrtstrecke und eingesetzter Fahrer) des eingesetzten GPS-Systems in diesem Zusammenhang war nicht ersichtlich. Aufgrund der fehlenden Rechtsgrundlage lag somit eine

unzulässige Nutzung des GPS-Systems und der dadurch generierten personenbezogenen Daten zu Kontrollzwecken vor. Der TLfDI forderte die Stadtwerke auf, ab sofort das GPS-System nur im Einklang mit dem Datenschutz zu nutzen. Dazu setzte der TLfDI eine Frist, innerhalb derer die Stadtwerke mitteilen sollten, welche Maßnehmen sie zur datenschutzkonformen Ausgestaltung des GPS-Systems treffen. Eine Reaktion der Stadtwerke blieb aus. Nach einer weiteren Erinnerung und dem Hinweis auf die Unterstützungspflicht gemäß § 38 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG), beanstandete der TLfDI die fehlende Unterstützung gemäß § 39 Abs. 1 Satz 1 ThürDSG. Im Nachgang zu dieser Beanstandung teilten die Stadtwerke mit, dass eine Speicherung der GPS-Daten nun nicht mehr erfolge. Somit sah der TLfDI den Fall zunächst als erledigt an. Doch der Beschwerdeführer wandte sich kurz danach erneut an den TLfDI und teilte mit, dass sich in den Fahrzeugen der Stadtwerke Schmölln GmbH noch immer GPS-Sender befänden. Der TLfDI nahm dies zum Anlass, vor Ort eine unangekündigte datenschutzrechtliche Kontrolle gemäß § 37 ThürDSG durchzuführen. Dabei überzeugte sich der TLfDI davon, dass die Speicherung der durch das GPS-System entstandenen Protokolldaten deaktiviert wurde.

Weiterhin stellte der TLfDI fest, dass man an den vier durch Passwort zugangsgesicherten Arbeitsplätzen nur sah, wo sich ein mit GPS ausgestattetes Fahrzeug der Stadtwerke aktuell befand. Zusätzlich konnte ein ereignisgesteuertes Bewegungsprofil für den aktuellen Tag zum jeweiligen Fahrzeug aufgerufen werden. Dieses Profil wurde täglich um 00:00 Uhr jeweils gelöscht. Damit war keine unzulässige Überwachung der Fahrzeugführer festzustellen. Die Möglichkeit, zu Zwecken der Flottenkontrolle (optimaler Einsatz des Fahrzeugs durch den jeweiligen Arbeitnehmer) und des Arbeitsschutzes (Überprüfung bei nicht erklärbaren unverhältnismäßig langen Aufenthalten an abgelegenen Arbeitsorten von nur einem Arbeitnehmer) ein GPS-System zu verwenden, rechtfertigt insoweit die Verarbeitung personenbezogener bzw. personenbeziehbarer Daten der Fahrzeugführer.

Ein Leistungsnachweis, für den nach der Betriebsanweisung eine Datenspeicherung für drei Monate als erforderlich angesehen wurde, um sporadisch und mitunter sehr zeitversetzt Rückfragen durch die Auftraggeber zum Nachweis der Leistungserbringung unter Nutzung der GPS-Daten beantworten zu können, war mangels Speicherung

nicht mehr möglich, aber nach den Angaben der Stadtwerke auch nicht (mehr) erforderlich. Die Stadtwerke machten im Rahmen der Vor-Ort-Kontrolle gegenüber dem TLfDI ihren Bedarf deutlich, über den Einsatz von GPS in Räumfahrzeugen im Winter weitergehende Daten (Zeitpunkt des Einsatzes des Schneeräumfahrzeugs und der Menge des ausgebrachten Streusalzes etc.) für eventuelle Nachfragen der Polizei bei Unfällen und Beschwerden von Bürgern wegen mangelhafter Erbringung des Winterdienstes für einen gewissen Zeitraum zu speichern. Nach § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Nach § 20 Abs. 1 ThürDSG ist das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Eine Erforderlichkeit der Erhebung der bezeichneten Daten und deren Speicherung für die vorgenannten Zwecke lag nach der Einschätzung des TLfDI insoweit vor. Er wies darauf hin, dass bei einer beabsichtigten Nutzung der Daten darauf zu achten sei, dass letztendlich kein Personenbezug zum Fahrer hergestellt werde, soweit dies nicht erforderlich sei. Zu prüfen sei weiterhin, wie lange diese Daten benötigt würden. Zudem müssten entsprechende Löschfristen festgelegt werden. Besondere Bedeutung käme in diesem Zusammenhang auch der Transparenz für die von der Datenerhebung und -verarbeitung betroffenen Mitarbeiter als Fahrzeugführer zu. In einer Betriebsanweisung müsse daher konkret aufgeführt werden, welche konkreten Angaben zu dem jeweiligen Fahrzeug erhoben und gespeichert würden. Auch eine Angabe zu einem Fahrzeug ist ein personenbezogenes Datum, wenn ihm eine natürliche Person als Fahrer zugeordnet werden kann. Weiterhin wies der TLfDI darauf hin, dass der konkrete Zweck der Erhebung und Speicherung sowie die Speicherungsfrist anzugeben seien. Die Speicherungsfrist ist daran zu messen, wie lange die Daten für die konkrete Aufgabenerfüllung erforderlich sind. Eine Leistungs- und Verhaltenskontrolle der Mitarbeiter ist grundsätzlich auszuschließen (§ 33 Abs. 4 ThürDSG). Für mögliche Ausnahmen, beispielsweise bei konkretem Verdacht auf Verletzung der Arbeitspflichten, müssten Kontrollbefugnisse (z. B. ein Vier-Augen-Prinzip) festgelegt werden. Dabei wäre auch zu beachten, dass der Zugriff auf die Kontrolldaten nur den zuständigen Mitarbeitern für den konkreten

Zweck, für den die Daten erhoben würden, zu erlauben sei. Da die Speicherung der Daten auch für eventuelle Nachfragen der Polizei erfolgen sollte, empfahl der TLfDI, Auskünfte bzw. Datenübermittlungen schriftlich zu dokumentieren. Der TLfDI bat die Stadtwerke, sofern sich diese zu einer Verarbeitung von Daten der Fahrzeuge des Räumdienstes im Winter entscheiden sollten, um eine Übersendung entsprechender Regelungen. Da dies bis zum Herbst 2015 nicht erfolgte, forderte der TLfDI die Übersendung dieser Unterlagen bei den Stadtwerken Schmölln ein. Die datenschutzrechtliche Prüfung dieses Falles ist also noch nicht abgeschlossen, sodass der TLfDI über das Ergebnis in seinem nächsten Tätigkeitsbericht informieren wird.

Ein unzulässiger Eingriff in das Persönlichkeitsrecht des Beschäftigten ist grundsätzlich dann gegeben, wenn der Mitarbeiter, losgelöst von einem bestimmten konkreten Informationsbedarf des Arbeitgebers, einer Rundumkontrolle seiner Bewegungen unterworfen sein würde. Damit verbietet sich auch grundsätzlich eine allgemeine Überwachung der Mitarbeiter zur Kontrolle des Verbotes privater Nutzung der Fahrzeuge. In Fällen eines unverhältnismäßig langen Aufenthaltes an abgelegenen Arbeitsplätzen kann durch telefonische Rückfragen oder Vor-Ort-Kontrollen geprüft werden, ob der Aufenthalt arbeitsbedingt begründet ist oder z. B. eine Verletzung der Arbeitspflicht des Beschäftigten vorliegt.

6.10 Bewerbungen per E-Mail

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) führte eine stichprobenmäßige Durchsicht von Stellenausschreibungen der Landesregierung durch. Dabei hat sich ein gemischtes Bild ergeben. Während in den meisten Geschäftsbereichen Bewerbungen per E-Mail (teilweise aus datenschutzrechtlichen Gründen) nicht erwünscht waren oder keine Berücksichtigung finden sollten, wurden in anderen Geschäftsbereichen Bewerbungen durch die Angabe von E-Mail-Adressen zugelassen. Die Angabe der E-Mail-Adressen konnte von potentiellen Interessenten als Aufforderung zur Bewerbung per E-Mail verstanden werden.
Der TLfDI nahm dies zum Anlass, die obersten Landesbehörden auf die nachfolgenden datenschutzrechtlichen Aspekte hinzuweisen und

bat darum, auch die nachgeordneten Bereiche hierüber zu informieren und bei zukünftigen Ausschreibungen zu beachten:
Kommt es aufgrund einer Bewerbung zu einer Beschäftigung, werden die von Bewerbern mit der Bewerbung eingereichten personenbezogenen Daten Bestandteil der Personalakten, für die die dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) gelten, die besondere Schutzvorschriften und Zugangsregelungen enthalten. Diese Bestimmungen finden gemäß § 33 Thüringer Datenschutzgesetz (ThürDSG) für Angestellte, Arbeiter und Auszubildende im öffentlichen Dienst entsprechend Anwendung. Den von den Bewerbern zum Zweck der Eingehung eines Dienstverhältnisses eingereichten personenbezogenen Daten kommt somit ein besonderer Schutzbedarf zu. Zugang zu diesen Daten dürfen nur damit betraute Personen haben (vgl. § 80 Abs. 1 ThürBG). Ein allgemeiner Zugang zu Bewerberdaten ist daher in den Behörden auszuschließen.
Sollen von öffentlichen Stellen Bewerbungen per E-Mail zugelassen werden, sind besondere technische und organisatorische Maßnahmen zu treffen, die unbefugte Kenntnis der Bewerbungsunterlagen ausschließen. Für den unversehrten Zugang der personenbezogenen Daten muss daher eine Verschlüsselung und Entschlüsselung möglich sein.
Weiterhin kann nicht das allgemeine Postfach eines Hauses genutzt werden, da die allgemeine Poststelle und Registratur mangels konkreter Aufgabenerfüllung zu diesen personenbezogenen Daten der Bewerber keinen Zugang/Zugriff haben darf.
Wie im Nachgang festzustellen war, wurden die Ausführungen bei daraufhin folgenden Stellenausschreibungen berücksichtigt. Die meisten Ressorts verfügen offenbar nicht über die erforderlichen Vorrichtungen zur Sicherstellung gegen unbefugte Kenntnisnahme, denn es findet sich nunmehr meistens der Zusatz, dass E-Mail-Bewerbungen aus datenschutzrechtlichen Gründen nicht erwünscht sind.

Bewerbungsunterlagen für Stellen im öffentlichen Dienst kommt ein besonderer Schutzbedarf zu. Stellenbewerber dürfen nur dann zur Einreichung von Bewerbungsunterlagen per E-Mail aufgefordert werden, wenn die Vertraulichkeit durch die öffentliche Stelle durch entsprechende technische und organisatorische Maßnahmen gewährleistet werden kann.

6.11 Elektronische Personalakte

Die dienstrechtlichen Vorschriften wurden mit Inkrafttreten zum 1. Januar 2015 dahingehend geändert, dass nunmehr nach § 81 Abs. 2 Satz 1 Thüringer Beamtengesetz (ThürBG) die Personalakten in Teilen oder vollständig auch automatisiert geführt werden können. Voraussetzung hierfür ist, dass die nach § 9 Thüringer Datenschutzgesetz (ThürDSG) erforderlichen technischen und organisatorischen Voraussetzungen vorliegen. Beabsichtigt eine öffentliche Stelle, die Personalakten zukünftig im Rahmen eines Dokumentenmanagementsystems automatisiert zu führen, sind verschiedene Aspekte zu beachten:

Allgemein muss in technischen Projekten, wie zur Einführung der elektronischen Personalakte in ein existierendes Dokumentenmanagementsystem, in der Dokumentation genau ausgeführt werden, welche Rollen eine Software vorsieht und wie diese Rollen mit Berechtigungen belegt werden. Rollen sind klar zu trennen und in ihrer funktionalen Beschreibung zu dokumentieren. Weiterhin ist schlüssig zu dokumentieren, welche Bereiche mit zugehörigen Mitarbeitern diesem Rollenkonzept zugewiesen werden und wer Änderungen an den Berechtigungen vornehmen darf. Sofern eine Person mehrere Rollen ausübt, sind ihr dafür grundsätzlich auch verschiedene Accounts in der Software zuzuweisen. Dies kann – abhängig von der inneren Struktur der jeweiligen Software – auch in Form der Zuweisung verschiedener „Werkzeuge“ zu ein- und demselben Account erfolgen. Wichtig ist aus datenschutzrechtlicher Sicht, dass jederzeit nachvollziehbar ist, wer welche Änderungen an Dokumenten einerseits, aber bspw. auch an Einstellungen des Systems andererseits vorgenommen hat. Die Rollen des Datenschutzbeauftragten sowie des/der IT-Administratoren sind personell voneinander zu trennen. Da Administratoren mit grundsätzlich unterschiedlichen Passwörtern arbeiten, sind Gruppenkennungen in einem Feinkonzept zur Rechtezuweisung grundsätzlich zu vermeiden.

Für die elektronische Personalaktenführung speziell gilt, dass absolut sichergestellt sein muss, dass auf die automatisiert geführten Dokumente der Personalakte ein unbefugter Zugriff oder unbefugter Zugang nicht möglich ist. Zugang dürfen nämlich nach wie vor nur die Beschäftigten haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur,

soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist (§ 80 Abs. 1 ThürBG). Daneben muss beachtet werden, dass der übergeordnete Administrator hier ebenfalls berücksichtigt werden muss, auch wenn er selbst als solcher, wenn er nicht auch mit der Bearbeitung von Personalangelegenheiten beauftragt ist, keinen Zugang zur Personalakte haben darf. Werden zur Anlegung der elektronischen Personalakte vorhandene Dokumente eingescannt, können damit nicht etwa Personen außerhalb der Personalverwaltung beauftragt werden. Das immer wieder weiterentwickelte PDF-Format erlaubt bspw. heute digitale Signaturen, Verschlüsselung und Passwortschutz. Es wird dringend empfohlen, gerade in Bezug auf abzulegende Personaldokumente, ein rechts- sowie revisionssicheres PDF-Format zu verwenden. Eine von vielen Fundstellen dazu sei hier zitiert
http://www.moderneverwaltung.sachsen.de/download/Handreichung_rechtssichere_Aufbewahrung_V1_2009.11.16.pdf

Weiterhin ist die Problematik der Urkundenqualität von elektronischen Dokumenten in diesem Zusammenhang noch nicht konkret geklärt. Daher ist es angeraten, Unterlagen mit Urkundenqualität auch noch in Papierform zu führen (so genannte Hybridakte). Kann zu einzelnen Unterlagen eine gesonderte Löschung aufgrund Fristablaufs im automatisierten Verfahren nicht vorgenommen werden, sind diese Dokumente ebenfalls besser in Papierform zu führen. Dies betrifft Krankmeldungen, Arbeitszeitdaten, Urlaubsgewährung, aber auch für Betroffene ungünstige Beschwerden und Behauptungen (§§ 86, 87 ThürBG). Näheres, auch zur teilweisen oder vollständig automatisiert geführten Personalakte, sollte in einer novellierten Personalaktenführungsrichtlinie geregelt werden.

Soll die Personalakte der Bediensteten bei öffentlichen Stellen zukünftig automatisiert geführt werden, sind umfangreiche Vorarbeiten durchzuführen. Es muss ein detailliertes Feinkonzept erarbeitet werden, das auch den besonderen Schutz der Personalaktendaten berücksichtigt. Den differenzierten Zugriffsrechten kommt dabei eine besondere Bedeutung zu.

6.12 Fingerabdruckscanner zur Arbeitszeiterfassung?

Vereinzelt wenden sich Beschäftigte und Betriebsräte Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil in ihrem Betrieb im Zuge der fortschreitenden Technisierung ein Fingerabdruckscanner zur Arbeitszeiterfassung eingeführt werden soll. Mit solchen Geräten zur Erfassung von Fingerabdrücken sind bisweilen ungute Vorstellungen und Befürchtungen verbunden, da man mit der Abgabe von Fingerabdrücken oftmals polizeiliche Maßnahmen vor Augen hat. Fingerabdrücke müssen doch meist nur Verbrecher abgeben …
Zur datenschutzrechtlichen Problematik des Einsatzes eines Fingerabdruckscanners bei der Arbeitszeiterfassung verweist der TLfDI auf die „Hinweise zur biometrischen Datenerfassung am Arbeitsplatz“, die auf seiner Homepage unter Themen – Beschäftigtendatenschutz verfügbar sind. Folgendes ist zu beachten:

1. Die Erhebung, Speicherung, Übermittlung und Nutzung biometrischer Daten stellt grundsätzlich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Arbeitnehmer dar. Er ist gemäß § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Biometrische Daten gelten dabei als besonders sensible Daten, die einer besonderen Schutzbedürftigkeit unterliegen.
2. Es existieren für die Arbeitnehmer weit weniger in das Recht auf informationelle Selbstbestimmung eingreifende und dem Grundsatz der Datensparsamkeit nach § 3a BDSG gerecht werdende technische wie organisatorische Möglichkeiten, die geeignet sind, die Arbeitszeit zu erfassen und dabei ohne die Verwendung biometrischer Daten auszukommen. Das sind beispielsweise Arbeitszeiterfassungssysteme, die mit einer Chipkarte oder einem Transponder zu bedienen sind. In manchen Betrieben reicht auch die handschriftliche Aufzeichnung aus.
3. Allein die geringere, aber auch nicht auszuschließende Betrugsanfälligkeit, Arbeitszeiten zu manipulieren, führt im Rahmen einer Verhältnismäßigkeitsprüfung nicht zu einer anzunehmenden Erforderlichkeit der Verwendung biometrischer Daten zur Arbeitszeiterfassung. Es kann regelmäßig nicht davon ausgegangen werden, dass Arbeitnehmer sich rechtswidrig verhalten. Im Falle

festgestellter Falschangaben von Arbeitszeiten stehen dem Arbeitgeber genügend Mittel zur Vertretung eigener Interessen (z. B. strafrechtliche Verfolgung wegen Betruges gemäß § 263 StGB und außerordentliche Kündigung) zur Verfügung.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auch biometrischer Daten, ist gemäß § 4 Abs. 1 BDSG unter anderem dann zulässig, wenn der von der Datenverarbeitung Betroffene einwilligt. Die Einwilligung ist aber nur unter den Voraussetzungen des § 4a BDSG wirksam, d. h., wenn diese schriftlich und tatsächlich freiwillig abgegeben und der Betroffene auf die Folgen einer verweigerten Einwilligung hingewiesen wird. Insbesondere in bestehenden Abhängigkeitsverhältnissen, wie im Rahmen arbeitsvertraglicher Beziehungen, ist die Frage der Freiwilligkeit regelmäßig kritisch zu hinterfragen. Hier müssen die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten umfassend informiert werden. Außerdem muss es eine tatsächliche Alternative zu der biometrischen Zeiterfassung geben, sodass der betroffene Arbeitnehmer ein Wahlrecht hat. Diese kann beispielsweise darin bestehen, dass neben der Zeiterfassung mittels Fingerabdruck die Erfassung über Transponder angeboten wird.

Die mit dem Einsatz eines biometrischen Systems zur Arbeitszeiterfassung verbundene Problematik ist in den „Hinweisen zur biometrischen Datenerfassung am Arbeitsplatz“ dargelegt und auf der Homepage des TLfDI abrufbar.

6.13 Fragebögen zur Mitarbeiterbefragung

Wie steht es mit der Zufriedenheit der Beschäftigten? Gibt es Missstände? Besteht Verbesserungsbedarf oder ist alles in Ordnung? Qualitätsmanagement nimmt in der heutigen Zeit einen hohen Stellenwert ein. Und am Anfang steht meistens eine Befragung der Betroffenen, die möglichst eine ehrliche Einschätzung abgeben sollen, damit alles (noch) besser werden kann.

Für die Aussagekraft einer Befragung ist es wichtig, dass die Betroffenen wegen ihrer Offenheit keine Nachteile befürchten müssen. Das beste Mittel dafür ist die anonyme Befragung. Dabei reicht es nicht aus, dass lediglich auf die Angabe des Namens verzichtet wird. Sollen Geschlecht, Alter, Dauer der Betriebszugehörigkeit und konkreter Tätigkeitsbereich (Abteilung, Sachgebiet etc.) angegeben

werden, bedarf es unter Umständen nur noch weniger weiterer Angaben und der Auskunftserteilende wird als Person zumindest bei interner Auswertung mit etwas Zusatzwissen wieder erkennbar, insbesondere, wenn in seinem Tätigkeitsbereich nur wenige Personen beschäftigt sind. Anonymität für die Betroffenen bedeutet, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (vgl. § 3 Abs. 9 Thüringer Datenschutzgesetz – ThürDSG). Kann ein einzelner Fragebogen unter den geschilderten Umständen einer Person zugeordnet werden, sind Maßnahmen zu treffen, dass diese Erkenntnisse nicht der Beschäftigungsstelle zur Kenntnis gelangen. Besonderes Augenmerk ist dann auf die Auswertung zu legen. Aus dem Gesamtergebnis der Befragung darf kein Rückschluss auf die einzelne Person mehr möglich sein. Dies wird in der Regel den Teilnehmern in einer Information versichert. Ob die Anonymität allerdings vollständig gewährleistet ist, wird bisweilen von den Teilnehmern bezweifelt. In solchen Fällen kann man sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wenden, wovon die Betroffenen im Berichtszeitraum regelmäßig Gebrauch machten.

Zu einer Mitarbeiterbefragung zur Arbeitszufriedenheit, der Arbeitsbelastung, zum Verhältnis zu Vorgesetzten und Kollegen und Ähnlichem in einer öffentlichen Stelle des Landes, die am Wettbewerb teilnimmt, und damit gemäß § 26 ThürDSG das Bundesdatenschutzgesetz (BDSG) Anwendung findet, hat der TLfDI auf eine Anfrage eines Betroffenen hin Folgendes ausgeführt:

Zwar blieb die Stellungnahme des Einzelnen in diesem Fall ohne Namen, gleichwohl konnte aber die Erhebung von personenbezogenen Daten aufgrund der Gestaltung des Fragebogens im Einzelfall bejaht werden. Insbesondere auf Seite 1 des Umfragebogens waren Angaben zu machen, welche sich auf die Abteilung, das Alter, Geschlecht und die Berufsgruppe des Befragten bezogen. Durch diese Einzelangaben über persönliche und sachliche Verhältnisse war der Befragte, auch ohne Angaben des Namens, zumindest bestimmbar i. S. v. § 3 Abs. 1 BDSG.

Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Ent-

scheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Die vorliegende Befragung sollte einer Zertifizierung nach DIN-Normen von Qualitätsmanagementsystemen dienen, auf deren Grundlage eine Leistungsverbesserung erreicht werden sollte. Dieser Zweck ist von der Erlaubnisnorm des § 32 BDSG gedeckt. Allerdings müssen bei der Befragung auch die schutzwürdigen Interessen der Beschäftigten beachtet werden. Eine Datenerhebung, -verarbeitung und -nutzung mittels einer Mitarbeiterbefragung ist daher grundsätzlich nur zulässig, wenn die nachfolgenden Voraussetzungen eingehalten werden:

1. Angaben und Ergebnis müssen hinreichend anonymisiert werden, sodass das Resultat der Befragung keinem konkreten Mitarbeiter mehr zugerechnet werden kann.
2. Die Teilnahme an der Befragung muss freiwillig sein.
3. Es dürfen den Mitarbeitern keine Sanktionen oder sonstigen Nachteile drohen, wenn keine Teilnahme an der Befragung erfolgt.
4. Der mittels der Umfrage verfolgte Zweck muss den Befragten im Fragebogen erläutert werden, und zudem darf das mittels Auswertung des Fragebogens gewonnene Resultat in Zukunft auch nur für diesen Zweck verwendet werden.
5. Die Befragten sind über den Ablauf und den Gegenstand der Befragung und darüber, durch wen und für wen die Daten erhoben und verarbeitet werden, zu informieren. Auch sollten die Beschäftigten darüber aufgeklärt werden, welche Auswertungen konkret vorgesehen sind.
6. Im Fragebogen selbst sind ausführliche Hinweise bezüglich der Einhaltung der in 1.–3. genannten Voraussetzungen zu machen. Die „Freiwilligkeit“ ist insbesondere durch eine drucktechnische Hervorhebung kenntlich zu machen.

Diese Voraussetzungen für die Zulässigkeit der Mitarbeiterbefragung waren durch Gestaltung des Fragebogens weitgehend eingehalten. Es bedurfte jedoch noch der drucktechnischen Hervorhebung des Hinweises auf die Freiwilligkeit der Teilnahme, des Hinweises, dass bei Nichtteilnahme keine Nachteile drohen und negative Antworten sanktionslos bleiben. Wesentliche Bedeutung kommt einer vorherigen umfassenden Aufklärung und Information der Mitarbeiter zu. Es sollte daher noch ausdrücklich darauf hingewiesen werden, dass sich der Mitarbeiter der Umfrage ohne potentielle Nachteile entziehen

kann. Ein solcher zusätzlicher Hinweis ist notwendig, um eine Freiwilligkeit der Teilnahme zu gewährleisten. Zudem war auch ein ausdrücklicher Hinweis im Fragebogen nicht enthalten, dass negative Beurteilungen des Vorgesetzten/des Unternehmens etc. ohne Konsequenzen für den Befragten bleiben. Dies ist erforderlich, um den Befragten nicht in einen Gewissenskonflikt zu bringen und unwahre positive Einschätzung als Antworten zu erzwingen. Zu guter Letzt bedurfte es eines Hinweises, dass Fragebögen nach Auswertung vernichtet werden, um nach Abschluss der Datenerfassung einen späteren Zugriff auf die Fragebögen sowie die damit verbundene Vorratsdatenspeicherung zu verhindern. Mithin wird somit auch sichergestellt, dass der einzelne Befragte auch weiterhin anonym bleibt.

Soll zum Zweck des Qualitätsmanagements eine Mitarbeiterbefragung durchgeführt werden, sind die Betroffenen vorab umfassend über das festgelegte Vorgehen zu informieren. Die Teilnahme muss freiwillig sein. Die Anonymität des Betroffenen ist sicherzustellen, nicht zuletzt auch, da nur anonyme Befragungen ein unverfälschtes Bild versprechen. Nach der Auswertung sind die Fragebögen zu vernichten.

6.14 Wenn sich Beschäftigte über andere Beschäftigte beschweren: ein Datenschutzproblem?

Eine Mitarbeiterin eines Landesamtes beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie sich beim Umgang mit ihren personenbezogenen Daten als Beschäftigte in der Dienststelle in ihren schutzwürdigen Belangen beeinträchtigt sah. Der Amtsleiter hatte nämlich von einem anderen Mitarbeiter des Amtes E-Mails erhalten, in denen dieser sich über die Beschwerdeführerin beklagte. Hierzu hatte sie Auskunft darüber verlangt, was denn der Mitarbeiter über sie behaupte, denn sie war diesbezüglich zu einem Mitarbeitergespräch einbestellt und auch von anderen Mitarbeitern des Amtes darauf angesprochen worden. Die Dienststelle teilte ihr daraufhin mit, dass es sich um eine rein persönliche Angelegenheit handle, die die Beschwerdeführerin doch bitte privat zu klären hätte. Einen Auskunftsanspruch erkannte das Amt nicht an.

Der TLfDI, der nebenbei aufgrund der geäußerten Befürchtungen der Beschwerdeführerin wegen dienstlicher Nachteile darauf hinwies, dass nach § 11 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) niemand benachteiligt oder gemaßregelt werden dürfe, weil er von seinem Recht, sich an den TLfDI zu wenden, Gebrauch gemacht hat, fragte beim Amtsleiter nach. Der angesprochene Amtsleiter erläuterte, er wolle unbedingt vermeiden, dass private Auseinandersetzungen ins Amts getragen und am Arbeitsplatz – eventuell unter Einbeziehung von Arbeitskollegen – zum Nachteil der Arbeitsleistung und des Amtsfriedens ausgefochten werden. Es sei richtig, er habe als Leiter des Amtes – persönlich – E-Mails eines Beschäftigten erhalten. Den Inhalt, der keinen dienstlichen Bezug aufwies, habe er zur Entscheidung zum weiteren Vorgehen mit dem örtlichen Personalrat, der Leiterin der Personalverwaltung und dem Datenschutzbeauftragten vertraulich erörtert. Zu diesem Zweck habe er die E-Mails ausgedruckt und in seinem elektronischen Postfach gelöscht. Weil aber die ihm unaufgefordert zugesandten und von ihm unerwünschten E-Mails auch besonders zu schützende personenbezogene Daten des Absenders enthielten, könne er sie der Beschwerdeführerin nicht zugänglich machen, weil sonst das datenschutzrechtliche Interesse des Absenders massiv verletzt wäre.
Der TLfDI legte gegenüber dem Amtsleiter dar, dass die Erörterung des Inhalts mit den genannten Funktionsträgern zur weiteren Vorgehensweise keinen grundsätzlichen datenschutzrechtlichen Bedenken begegnete. Die Äußerungen des Absenders waren zwar gegenüber dem Amtsleiter persönlich, aber dennoch in dessen Eigenschaft als Leiter der Behörde getätigt worden und somit der öffentlichen Stelle zuordenbar. Durch die dienstliche Erörterung mit den genannten Funktionsträgern kam den E-Mails auch eine dienstliche Behandlung zu, auch wenn letztendlich ein dienstlicher Bezug des Inhalts verneint worden war. Damit unterlagen die die Beschwerdeführerin betreffenden personenbezogenen Daten der Auskunftspflicht nach § 13 ThürDSG bzw. § 33 ThürDSG i. V. m. § 85 Abs. 4 Thüringer Beamtengesetz. Die personenbezogenen Daten, die der Absender dem Amtsleiter gegenüber von sich selbst offenbart hatte, konnten – wie richtig erkannt wurde – als Daten Dritter grundsätzlich nicht beauskunftet werden; insoweit kommt eine Schwärzung der Daten Dritter in Betracht.
Auch die weitere Aufbewahrung der E-Mails in Papierform war ein Problem. Sie stellte nämlich weiterhin eine Verarbeitung personen-

bezogener Daten dar (§ 3 Abs. 3 Nr. 2 ThürDSG). Da ein dienstlicher Bezug verneint worden war, waren die personenbezogenen Daten, die mit den E-Mails zur Kenntnis gelangten, für die (weitere) Aufgabenerfüllung der Stelle nicht erforderlich. Mangels des Vorliegens der Zulässigkeitsvoraussetzungen dürfen die Daten auch nicht weiter verarbeitet werden. Die E-Mails waren deshalb nach § 16 Abs. 1 Nr. 1 ThürDSG auch in Papierform zu löschen. Jedoch musste die Löschung unterbleiben, solange dem Auskunftsbegehren der Beschwerdeführerin noch nicht nachgekommen wurde.
Der Amtsleiter tut sich aber offenbar immer noch schwer, der Beschwerdeführerin eine entsprechende Auskunft zu geben und hat die E-Mail-Ausdrucke zur weiteren Prüfung, wie weit der Auskunftsanspruch gehe, erst mal dem TLfDI übersandt. Die Prüfung hierzu ist noch nicht abgeschlossen.

Schwärzt ein Beschäftigter aufgrund von privaten Streitigkeiten einen anderen Beschäftigten beim Amtsleiter an und ergibt sich keine Erforderlichkeit für dienstliche Reaktionen, sind die übermittelten personenbezogenen Daten mangels weiterer Aufgabenerfüllung umgehend zu löschen. Werden die Informationen dennoch aufbewahrt, hat ein Betroffener nach § 13 ThürDSG selbstverständlich einen Anspruch auf Auskunft über die über ihn gespeicherten Daten.

6.15 Schutz: Daten oder Kanzlerin? – Datenübermittlung anlässlich des Besuchs der Bundeskanzlerin

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum Kenntnis darüber, dass die Landesentwicklungsgesellschaft Thüringen mbH (LEG) personenbezogene Daten von ihren Mitarbeiterinnen und Mitarbeitern an die Landespolizeiinspektion (LPI) Erfurt übermittelt habe. Dies geschah angeblich anlässlich der Vorbereitung des Besuchs der Bundeskanzlerin Angela Merkel in Erfurt im Februar 2014. Bei den übermittelten Daten habe es sich konkret um die Familiennamen und Kfz-Kennzeichen jener Mitarbeiter gehandelt, welche üblicherweise die Tiefgarage unterhalb des LEG-Dienstgebäudes in Erfurt nutzen.
Zur Sachverhaltsaufklärung wandte sich der TLfDI im Rahmen seiner Kontrollbefugnis gemäß § 37 Thüringer Datenschutzgesetz

(ThürDSG) umgehend an die LEG. Von dieser erhielt er die Auskunft, dass die Übermittlung auf ein Ersuchen der LPI Erfurt erfolgt sei, und die betroffenen Mitarbeiter zudem per E-Mail über den Vorgang informiert worden wären.
Daraufhin richtete der TLfDI seine Kontrolltätigkeit nunmehr auf die LPI aus und erhielt von ihr eine umfassende Stellungnahme. Darin führte die LPI aus, dass nicht nur die Bundeskanzlerin, sondern auch weitere Veranstaltungsgäste von Seiten des Bundeskriminalamtes (BKA) als gefährdete Schutzpersonen eingestuft seien. Bei der Teilnahme solcher Personen gelten grundsätzlich die höchste Gefährdungsstufe sowie die Veranlassung weitreichender Schutzmaßnahmen. Diese Maßnahmen sollten gewährleisten, dass mögliche Störungen, Angriffe, Sabotageakte und Anschlagsfälle auf Personen und relevante Gebäude verhindert werden.
Aufgrund der baulichen Gegebenheiten – die Tiefgarage befindet sich unter dem Hotel, in dem die Kanzlerin und weitere Veranstaltungsgäste übernachteten – wurde die Tiefgarage als relevantes Gebäude betrachtet und musste daher entsprechend abgesichert werden.
Die polizeiliche Absicherung umfasste das Identifizieren potenzieller Gefährder und das frühzeitige Erkennen etwaiger Straftäter. Hierbei beurteilt die Polizei unter Berücksichtigung von Lagefeldern wie Raum, Zeit, Bedrohung, Gefahren, Politik, Staatsschutz usw. die polizeiliche Lage und trifft zur Gefahrenminimierung sowohl vor als auch während der Veranstaltung die erforderlichen Maßnahmen. Dazu gehört der Personen- und Objektschutz in allen denkbaren Facetten, aber auch das Prüfen und Organisieren von Zu- und Abfahrtsmöglichkeiten und Einlasskontrollen. In diese polizeilichen Maßnahmen war das Überprüfen und Sichern der Räume des Aufenthalts gefährdeter Personen sowie von Personen, die ggf. mit gefährdeten Personen in Kontakt treten und sich in ihrer unmittelbaren Umgebung aufhalten konnten, einzuordnen.
§ 31 Abs. 1 Polizeiaufgabengesetz (PAG) regelt als die spezielle Rechtsgrundlage die Grundsätze der Datenerhebung durch die Polizei und schreibt vor, dass die Datenerhebung durch Gesetz oder besondere Rechtsvorschriften zugelassen sein muss.
Die Polizei ist nach § 14 Abs. 1 Nr. 3 Thüringer Polizeiaufgabengesetz (PAG) dazu ermächtigt, die Identität einer Person festzustellen, wenn diese sich unter anderem in oder in unmittelbarer Nähe von einem besonders gefährdeten Objekt aufhält. Die Datenerhebung hat gemäß § 31 Abs. 2 Satz 1 PAG grundsätzlich beim Betroffenen

selbst zu erfolgen. Im vorliegenden Fall wurde die Datenerhebung aber über die LEG betrieben. Eine Datenerhebung bei Behörden, öffentlichen Stellen oder bei Dritten ist jedoch gemäß § 31 Abs. 2 Satz 2 PAG ausnahmsweise zulässig, wenn die Datenerhebung beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder die Erfüllung der polizeilichen Aufgaben gefährdet würde. Diese Voraussetzungen waren hier im konkreten Fall gegeben: Zum einen hätte bei einer Direkterhebung die Polizei jeden einzelnen Mitarbeiter der LEG / Tiefgaragennutzer überprüfen müssen, was ein unverhältnismäßiger Aufwand gewesen wäre, und zum anderen geschah die Datenerhebung auch offen im Sinne von § 14 Abs. 3 PAG. Die betroffenen LEG-Mitarbeiter wurden ja, wie bereits erwähnt, per E-Mail über die Datenerhebung in Kenntnis gesetzt.
Durch den Abgleich der Kennzeichen und Nachnamen der üblichen Tiefgaragennutzer konnte zudem eine Vollsperrung der Tiefgarage vermieden werden. Da eine Vollsperrung die berechtigten Nutzer sowohl in ihrer Handlungsfreiheit als auch in ihren Nutzungsrechten an den gemieteten Stellplätzen maximal eingeschränkt hätte, war die Beschränkung auf eine Berechtigungskontrolle eindeutig das mildere, aber gleichwohl effektive Mittel, um den Sicherungszweck hier zu erreichen.
Im Ergebnis konnte durch diese permanente polizeiliche Kontrolle der Tiefgaragenzufahrt im Interesse der Berechtigten und zur Entlastung der Bürger eine Vollsperrung des näheren Umfeldes vermieden werden.
Die erhobenen Daten waren zur Sicherung der Veranstaltung und der daran teilnehmenden Personen auch erforderlich. Die Aufnahme von Personalien ist polizeirechtlich eines der mildesten Mittel zur Gefahrenabwehr. Es schränkt die Betroffenen kaum fühlbar in ihren Grundrechten und in ihrer allgemeinen Handlungsfreiheit ein, ermöglicht aber auch eine effektive Abwehr oder Verhinderung rechtswidrigen Handelns.
Ein milderes, gleich geeignetes Mittel stand somit zur polizeilichen Aufgabenerfüllung nicht zur Verfügung, um eine Übersicht allgemein zutritts-/zufahrtsberechtigter LEG-Mitarbeiter zu erhalten.

Zur polizeilichen Aufgabenerledigung wurden personenbezogene Daten weiterhin von Mitarbeitern der übrigen benachbarten Firmen über einen Ansprechpartner erhoben. Die betreffenden Mitarbeiter hatten in gleicher Form eine Zufahrts-/Zutrittsmöglichkeit zur Tief-

garage, sodass die dargestellten rechtlichen Ausführungen für sie entsprechend galten.
Ein Verstoß gegen Bestimmungen des Datenschutzes, insbesondere des PAG, lag hier somit nicht vor.

Im Zuge einer effektiven Gefahrenabwehr kann die vorübergehende Einschränkung von Grundrechten vonnöten sein. Von dieser Möglichkeit ist freilich stets restriktiv, also mit äußerster Zurückhaltung, Gebrauch zu machen. Das Grundrecht auf informationelle Selbstbestimmung wird unter anderem durch § 31 Abs. 2 PAG dann eingeschränkt, wenn eine Erhebung personenbezogener Daten nicht direkt beim Betroffenen, sondern auch bei Behörden oder Dritten für zulässig erklärt wird. Dies ist gemäß § 31 Abs. 2 Satz 2 PAG zulässig, wenn die Direkterhebung beim Betroffenen nur mit unverhältnismäßig hohem Aufwand möglich ist oder die Erfüllung der polizeilichen Aufgaben gefährdet würde. Darüber hinaus ist die übermittelnde Stelle in einer solchen Fallkonstellation auch zur Datenübermittlung gemäß § 21 Abs. 1 Nr. 2 in Verbindung mit § 20 Abs. 2 Nr. 1 ThürDSG befugt.

6.16 Verfahren „Interamt“ (Onlineverfahren mit Speicherung und Verarbeitung der Bewerberdaten)

Die Thüringer Landesfinanzdirektion (TLFD) übersandte ein Verfahrensverzeichnis nach § 10 Thüringer Datenschutzgesetz (ThürDSG) für das Verfahren „Interamt" an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Kenntnis, um ihrer Unterrichtungspflicht nach § 8 Abs. 2 Satz 2 Thüringer Datenschutzgesetz (ThürDSG) nachzukommen. Grund für die Unterrichtung der TLFD als Auftraggeberin war der Abschluss eines Vertrages zur Nutzung einer Stellenplattform „Interamt.de“ in Auftragsdatenverarbeitung für das Bewerbungsverfahren für den Vorbereitungsdienst der Thüringer Steuerverwaltung 2014. Das Verfahren dient hauptsächlich der Bewerbungsdatenaufnahme und der Bewerberkommunikation, wobei die Bewerber ihre Daten selbst eingeben. Der TLfDI prüfte die von der TLFD übersandten Formblätter und merkte Folgendes an:
In dem Verfahren „Interamt" konnte beim Einstellen einer Stellenanzeige auch die Art der Bewerbung (in Papierform, per E-Mail oder unter Nutzung der Stellenplattform „Interamt.de") festlegt werden.

Insbesondere hat die TLFD für die Bewerbungen der Anwärter im mittleren und gehobenen Dienst in der Thüringer Steuerverwaltung für das Einstellungsjahr 2014 neben der Bewerbung in Papierform auch die Online-Bewerbung unter Nutzung der Stellenplattform „Interamt.de“ zugelassen. Dabei musste sich der Stellenbewerber bei der Nutzung der Stellenplattform „Interamt.de“ unter „Mein Interamt“ registrieren. Nach erfolgreicher Registrierung konnte der Nutzer seine Bewerbungen komplett erstellen und bei zugelassener Online-Bewerbung auch absenden. Das Verfahren sah außerdem vor, dass bei Eingang von Papierbewerbungen die Bewerber per Mail aufgefordert werden sollten, sich online auf der Seite https://www.interamt.de/koop/app/ zu bewerben.

Ergänzend bat der TLfDI um Stellungnahme, welche technisch-organisatorischen Maßnahmen die TLFD getroffen hat, um die Online-Bewerbung datenschutzgerecht zu gestalten. Daraufhin übermittelte die TLFD dem TLfDI den Vertrag mit der Auftragnehmerin über die Nutzung der Stellenplattform „Interamt.de“ samt der getroffenen technischen und organisatorischen Maßnahmen im Sinne des § 9 ThürDSG.

Die gesamte Datenübertragung erfolgte demnach verschlüsselt über „https“, was auch als technische Maßnahme nach § 9 ThürDSG vertraglich geregelt war. Nach Ablauf der Bewerbungsfrist wurde die Stellenausschreibung nicht mehr angezeigt. Eine Online-Bewerbung war dann nicht mehr möglich. Darüber hinaus teilte die TLFD noch mit, dass bereits vor der Einstellung der Stellenausschreibungen als Anwärter im mittleren und gehobenen Dienst in der Thüringer Steuerverwaltung für das Einstellungsjahr 2014 auf der Stellenplattform „Interamt.de“ eine Vielzahl von Bewerbungen in Papierform eingegangen war. Die Online-Bewerbung jedoch sei erst später möglich gewesen. Bei der Nutzung von „Interamt.de“ können Bewerber-Dateien automatisch erstellt werden. Des Weiteren kann beim Nutzen der Stellenplattform „Interamt.de“ genau vorgegeben werden, welche Bewerbungskriterien vom Bewerber zwingend ausgefüllt werden müssen. Daher forderte die TLFD die Bewerber, die sich vor dem Einsatz des Verfahrens bereits in Papierform beworben hatten, auf, sich nochmals online zu bewerben.

Nach den übersandten Unterlagen werden die Daten der Bewerber nach Abschluss des Verfahrens gelöscht, was regelmäßig zum 30. August eines jeden Jahres der Fall ist. Vor diesem Termin können Bewerbungen gelöscht werden, falls die erforderlichen Voraussetzungen für die Ausbildung von einem Bewerber nicht erbracht werden.
Aufgrund dieser Ausführungen der TLFD sah der TLfDI keine weiteren Bedenken gegen die vertraglich vereinbarte Auftragsdatenverarbeitung.

Nutzt eine öffentliche Stelle ein externes Online-Portal, um Online-Bewerbungen für ihre Stellenausschreibungen zu ermöglichen, bleibt sie gemäß § 8 Abs. 1 ThürDSG verantwortliche Stelle und muss somit die technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG vertraglich sicherstellen. Dabei müssen die zu übermittelnden Daten hinreichend vor unbefugtem Zugriff entsprechend dem jeweiligen Stand der Technik durch geeignete Verschlüsselungsverfahren geschützt werden.

6.17 Datenschutz im Stadtrat – was darf bei Disziplinarverfahren übermittelt werden?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Eingabe einer Angestellten einer Stadtverwaltung in Thüringen. Im Rahmen einer arbeitsrechtlichen Auseinandersetzung wurde der Angestellten durch den Bürgermeister eine E-Mail der Kommunalberatung, welche ihren Arbeitgeber – die Stadtverwaltung – datenschutzrechtlich betreut, ausgehändigt. Diese E-Mail enthielt am Ende eine eindeutige Belehrung dahingehend, dass „der Inhalt der Nachricht vertraulich ist und nur für den angegebenen Empfänger bestimmt ist. Jede Form der Kenntnisnahme oder Weitergabe durch Dritte ist unzulässig.“ Die Angestellte bat daher den TLfDI, zu prüfen, inwieweit die Weitergabe der „vertraulichen“ E-Mail der Kommunalberatung an sie als Dritte datenschutzrechtlich zulässig war. Weiterhin fragte die Angestellte den TLfDI, ob es aus datenschutzrechtlicher Sicht rechtens war, im nicht-öffentlichen Teil einer Stadtratssitzung ihre Disziplinarmaßnahme und ihren Namen konkret zu nennen.
Für die datenschutzrechtliche Beurteilung der Weitergabe der vertraulichen E-Mail durch den Bürgermeister an die Angestellte ist der

Inhalt des Thüringer Datenschutzgesetzes (ThürDSG) maßgeblich. Dieses kann durch eine private Einfügung von Text in eine E-Mail nicht abgedungen werden. Nach § 22 ThürDSG ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn sie entweder zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden oder der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlungen hat. Hinsichtlich der Übermittlung der E-Mail an die Angestellte der Stadtverwaltung durch ihren Arbeitgeber mit dem Hinweis, dass der Inhalt der Nachricht vertraulich sei, konnte der TLfDI aber keinen datenschutzrechtlichen Verstoß feststellen. Vorliegend hatte die Angestellte wegen der laufenden arbeitsrechtlichen Auseinandersetzung mit ihrem Arbeitgeber aber ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten.

Hinsichtlich der Nennung des Namens und der Disziplinarmaßnahme der Angestellten im nicht-öffentlichen Teil einer Stadtratssitzung, stellte der TLfDI zunächst fest, dass nach § 32 Abs. 1 der Thüringer Kommunalordnung (ThürKO) der Stadtrat und der Bürgermeister Organe der Gemeinde sind. Der Stadtrat beschließt über die Aufgaben des eigenen Wirkungskreises, soweit nicht der Bürgermeister zuständig ist. Nach § 29 Abs. 3 ThürKO ist der Bürgermeister die oberste Dienstbehörde der Beamten der Gemeinde. Er ist Vorgesetzter und Dienstvorgesetzter der Gemeindebediensteten. Der Bürgermeister benötigt für die in § 29 Abs. 3 Satz 3 ThürKO genannten Personalentscheidungen die Zustimmung des Gemeinderates oder des zuständigen Ausschusses. Der von der Angestellten geschilderte Fall, die Kundgabe ihres Namens sowie die Benennung der Disziplinarmaßnahme, gehörte aber nicht zu den in § 29 Abs. 3 Satz 3 ThürKO genannten Fällen. Insofern bestand auch keine Berichtspflicht des Bürgermeisters nach § 22 Abs. 3 Satz 3 ThürKO. Allerdings gibt § 22 Abs. 3 Satz 4 ThürKO dem Gemeinderat ein Recht auf Auskunft. Dieses Auskunftsrecht gilt jedoch nicht für Angelegenheiten, die der Bürgermeister nach § 29 ThürKO in eigener Zuständigkeit erledigt. Der Gemeinderat hat in diesen Fällen keinerlei Einflussmöglichkeiten, nicht einmal einen Informationsanspruch (so

Uckel/Hauth/Hoffmann/Noll, Kommunalrecht in Thüringen, Rechtssammlung, § 22 ThürKO, Nr. 8, S. 10).
Im Ergebnis war damit der Bürgermeister dem Stadtrat in der Angelegenheit der Angestellten keinerlei Rechenschaft schuldig. Mithin lag im Vorgehen des Bürgermeisters ein datenschutzrechtlicher Verstoß vor. Soweit die Angestellte den TLfDI danach fragte, ob Fristen bei einem möglichen Vorgehen gegen die Handlungen des Bürgermeisters zu wahren wären, teilte dieser der Angestellten mit, dass es für eine datenschutzrechtliche Prüfung durch den TLfDI keine gesetzliche Frist gebe. Das Ergebnis wurde der Angestellten mitgeteilt, eine Rückmeldung, ob der TLfDI weiter tätig werden soll, erfolgte bisher nicht.

Nach § 22 ThürDSG ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn sie entweder zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden oder der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlungen hat. Der Bürgermeister benötigt für die in § 29 Abs. 3 Satz 3 ThürKO genannten Personalentscheidungen die Zustimmung des Gemeinderates oder des zuständigen Ausschusses. Die Benennung einer Disziplinarmaßnahme gehörte aber nicht zu den in § 29 Abs. 3 Satz 3 ThürKO genannten Fällen.

6.18 Geheime Personalakten?

Ein Beschäftigter war zu einer Dienststelle im Geschäftsbereich einer obersten Landesbehörde zunächst abgeordnet und später übernommen worden. Nun befand er sich in Rechtstreitigkeiten wegen verschiedener Personalangelegenheiten mit seiner personalverwaltenden Stelle. Er stellte fest, dass dem Gericht weit mehr Unterlagen mit personenbezogenen Daten über ihn als Beschäftigten vorgelegt worden waren, als ihm im Rahmen der Einsicht in seine Personalakte bei der Beschäftigungsbehörde zuvor zur Verfügung standen. Daher wandte er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er nun davon ausging, dass über ihn neben der offiziellen Personalakte geheime Per-

sonalunterlagen geführt wurden und darüber hinaus aus seiner Sicht wesentliche Unterlagen in der Personalakte fehlten.
Der TLfDI führte daraufhin in der Beschäftigungsbehörde eine datenschutzrechtliche Kontrolle gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) durch und ließ sich sämtliche Personalunterlagen und Sachvorgänge, die personenbezogene Daten des Betroffenen als Beschäftigten enthielten, zur Einsicht vorlegen. Die Kontrolle wurde nicht vorher angekündigt, um jeglichen Manipulationsverdacht zu vermeiden. Der Überraschungseffekt einer unangekündigten Kontrolle hat den Vorteil, dass der Sachverhalt seitens der kontrollierten Stelle nicht vorbereitet werden kann. Der Stand der Aktenführung spiegelt dann im Regelfall das wider, was Beschwerdeführer vorgefunden hatten. Gleichzeitig besteht aber andererseits für die Kontrolle der Nachteil, dass auskunftsfähige Ansprechpartner eventuell nicht zur Verfügung stehen oder zwischenzeitliche Ereignisse die Verfügbarkeit der Unterlagen beeinträchtigen konnten. Bei dieser Kontrolle lagen aber keine derartigen Schwierigkeiten vor. Die Personalakte nebst eventueller Sachvorgänge war ausweislich der Anforderung durch das für die Rechtsstreitigkeiten zuständige Gericht abgefordert worden. Von den Unterlagen waren Kopien gefertigt worden, die dem TLfDI anstandslos vorgelegt wurden. Dabei stellte der TLfDI verschiedene Mängel hinsichtlich der Personalaktenführung fest.
Nach § 33 Abs. 1 ThürDSG gelten die §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) für das Verarbeiten oder Nutzen personenbezogener Daten über im öffentlichen Dienst beschäftigte Personen, die nicht verbeamtet sind, entsprechend, es sei denn besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Danach ist für jede Beamtin und jeden Beamten eine Personalakte zu führen. Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktenakten). Die Personalakte ist vertraulich zu behandeln. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein, wobei landesrechtlich hierzu Ausnahmen vorgesehen werden können.
Ergänzend zu den dienstrechtlichen Vorschriften kann die Personalaktenführungsrichtlinie (ThürStAnz 1998, S. 1812 ff.) sinngemäß herangezogen werden, auch wenn diese aufgrund der zum

1. Januar 2015 in Kraft getretenen Änderung der beamtenrechtlichen Vorschriften zu überarbeiten ist.
Neben der Personalakte können auch Sachvorgänge zu Bediensteten geführt werden, sofern die zugrundeliegenden Sachverhalte sachlich zu trennen sind. Dies betrifft insbesondere Vorgänge, die im Rahmen der Aufsicht oder zur Rechnungsprüfung angelegt werden, Prüfungs-, Sicherheits- und Kindergeldakten sowie Daten über ärztliche und psychologische Untersuchungen und Tests mit Ausnahme ihrer Ergebnisse (§ 81 Abs. 1 Satz 2 ThürBG). Prozessakten und Vorgänge zu Widerspruchsverfahren zählen ebenso zu derartigen Sachakten. Nach deren Abschluss ist zu prüfen, ob das Ergebnis unmittelbar Auswirkungen auf das Dienstverhältnis hat und damit zur Personalakte zu nehmen ist.
Zuoberst war in der Akte ein amtsärztliches Gutachten offen eingelegt. In der Akte befanden sich noch weitere ärztliche Gutachten. Auch wenn zum Zweck der Personalverwaltung eine Kopie der dem Gericht vorgelegten Personalakte gefertigt wird, ist mit amtsärztlichen Gutachten ebenso zu verfahren, als ob sie im Original vorhanden wären, sie sind nämlich in verschlossenen Umschlägen zur Personalakte zu nehmen. Darüber hinaus dürfen nur die Ergebnisse der Eignungsuntersuchung und dabei festgestellte Risikofaktoren zur Personalakte gelangen, nicht aber umfängliche Gutachten mit der ganzen Familiengeschichte (Daten Dritter) und sämtlichen festgestellten Diagnosen und erhobenen Gesundheitsdaten. Selbst wenn der Beschäftigte selbst ärztliche Gutachten zur Personalakte gibt, weil er damit möglicherweise einen Nachweis führen will, muss die personalverwaltende Stelle derartige Unterlagen mit zu vielen Gesundheitsdaten zurückweisen. In der Akte fanden sich weiterhin verschiedene Dokumente, deren Erforderlichkeit für die Aufgabenerfüllung nicht oder nicht auf den ersten Blick erkennbar war. Erschwerend kam hinzu, dass die Personalakte von einer anderen personalführenden Stelle des Landes übernommen worden war und man sich scheute, Unterlagen, die definitiv für die Aufgabenerfüllung der neuen personalführenden Stelle nicht (z. B. Unterlagen, die mit der Bewerbung eingereicht wurden, wie Exmatrikulationsbescheinigung oder Kündigungsschreiben an einen früheren privaten Arbeitgeber) oder nicht mehr (alter Personalbogen mit Angaben zu den Eltern) erforderlich waren, zu entfernen. Also hatte man lediglich, wie von der Personalaktenführungsrichtlinie vorgeschrieben, ein Trennblatt eingelegt und etwas ungeordnet aktuelle Unterlagen dahinter gehef-

tet. Jedenfalls war die Personalakte anhand der vom TLfDI gegebenen Hinweise nach Rückgabe durch das Gericht zu überarbeiten.
Wie es dazu kam, dass der Beschwerdeführer weitere geheime Dokumente vermutete, war schnell geklärt. Das Gericht hatte nämlich nicht nur die Personalakte, sondern auch andere Vorgänge mit Beschäftigtendaten des Betroffenen abgefordert. Diese Unterlagen wurden nicht geheim geführt, denn auch in diese Akten oder Vorgänge hat ein Betroffener nach § 84 Abs. 4 ThürBG grundsätzlich ein Einsichtsrecht. Es gab einen Vorgang, der Unterlagen mit Notizen und Bemerkungen der unmittelbaren Vorgesetzten über den Beschwerdeführer enthielt. Diese Unterlagen waren über den nächsthöheren Vorgesetzten der Personalverwaltung zugeleitet worden, weil sich der Beschwerdeführer nicht nur mit der Personalverwaltung, sondern auch mit seinen Vorgesetzten und Kollegen kontrovers auseinandersetzte. Die Vorgesetzten sahen daher die Erforderlichkeit, sich über das dienstliche Verhalten und die Leistung des Beschwerdeführers Notizen zu machen, um sich abzusichern und gegebenenfalls rechtfertigen zu können.
Hierzu hat der TLfDI ausgeführt, dass grundsätzlich keine datenschutzrechtlichen Bedenken dagegen bestehen, soweit Dienstvorgesetzte sich zum Zweck der Beurteilung Notizen anfertigen und verschiedene Vorgänge als Gedankenstütze aufbewahren, um diese in die Beurteilung einzubeziehen. Für andere Zwecke dürfen die Notizen jedoch nicht genutzt werden. Eine Abbildung der Leistung und des Verhaltens des betreffenden Bediensteten entbehrt nach Erstellung einer Beurteilung der weiteren Erforderlichkeit zur Aufbewahrung. Somit sind die zum Zweck der Erstellung einer Beurteilung angefertigten Unterlagen zu löschen. Von Dienstvorgesetzten dürfen auch keine Kopien von Unterlagen, die sich auch in der Personalakte befinden, abgeheftet werden, weil dies eine unzulässige Führung einer Personalnebenakte darstellen würde. Werden Vermerke für die Personalverwaltung zum Zweck anstehender Personalmaßnahmen oder wegen anhängiger Rechtsstreitigkeiten gefertigt, können in einer Handakte hiervon grundsätzlich Entwürfe für einen kurzen Zeitraum aufbewahrt werden. Es ist jedoch darauf zu achten, dass sich daraus beim Dienstvorgesetzten kein Personalvorgang entwickelt, der das gesamte dienstliche Verhalten des Betroffenen dokumentiert. Die Führung eines solchen Vorgangs wäre nicht erforderlich und damit unzulässig.

Dem nächsthöheren Dienstvorgesetzten dürfen Dokumente und Schreiben über Bedienstete nur dann zugeleitet werden, wenn hierzu eine gesonderte Aufgabenstellung besteht. Werden Schreiben lediglich zur Personalverwaltung weitergeleitet, besteht keine Erforderlichkeit, dass die nächsthöheren Dienstvorgesetzten diese ebenfalls in Kopie aufbewahren.
Der TLfDI hat die Personalaktenführung nach § 39 ThürDSG beanstandet und die Dienststelle aufgefordert, nach Rückgabe der Unterlagen durch das Gericht die Personalakte anhand der gegebenen Hinweise zu überarbeiten. Dies hat die Stelle zugesagt. Zu gegebener Zeit wird der TLfDI dies überprüfen.

Zur Personalakte gehören alle Unterlagen, die einen Beschäftigten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Andere Unterlagen dürfen nicht zur Personalakte genommen werden. Die Personalakte kann in Grundakte und Teilakten gegliedert werden. Personalnebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur dann geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist. Neben der Personalakte können andere Akten (als Sachakten) existieren, die personenbezogene Daten über Beschäftigte enthalten, die für ihr Dienstverhältnis verarbeitet oder genutzt werden. Beschäftigte haben das Recht, in ihre Personalakte und grundsätzlich auch in die genannten anderen Akten Einsicht zu nehmen.

6.19 Lehrerdaten für die Schuljahresanalyse

An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde die Anfrage gerichtet, ob die Lehrer einer Fachschule zum Zweck der Schuljahresanalyse neben der breit gefächerten Aufschlüsselung ihrer Tätigkeit rund um den eigentlichen Unterricht (Vorbereitung, Einarbeitung, Betreuung von Projekten, Prüfungsaufsichten, Arbeitskorrekturen etc.) gegenüber der Schulleitung zum Zweck der Weiterleitung auch genau angeben müssten, aus welchen Gründen Fehltage angefallen waren. Als Fehltage waren in der hierfür von der Schule jeweils vorgesehenen Spalte krankheits-, urlaubs- und fortbildungsbedingte sowie sonstige freie Abwesenheitstage einzutragen. Wofür man das für welche Stelle letztendlich brauchte, war unklar, denn ein Betroffener hatte auf

seine entsprechende Anfrage an die Schulleitung keine zufriedenstellende Antwort erhalten.
Der TLfDI fragte bei der für die Fachschule zuständigen Landesanstalt nach, welchem Zweck die Datenerhebung diente, welche Maßnahmen zum Schutz der personenbezogenen Daten der Lehrer gegen unbefugte Kenntnis getroffen worden waren und ob geprüft worden sei, ob eine anonymisierte Erhebung ausreichte. Gleichzeitig äußerte er erhebliche Bedenken insbesondere gegen die Angabe der Krankheitstage.
Die Landesanstalt teilte mit, die Schuljahresanalyse werde von der Schulaufsicht nach den §§ 2 und 3 Thüringer Schulaufsichtsgesetz (ThürSchulAG) abgefragt. Hintergrund sei, auf diese Weise den sonstigen Einsatz der Lehrkräfte im laufenden Schuljahr planen zu können. Da es um den Einsatz einzelner konkreter Lehrpersonen gehe, sei eine Erhebung in anonymisierter Form nicht zielführend. Die Daten würden von jedem Lehrer abgefragt, von der Schulleitung zusammengefasst und danach an die obere Schulaufsicht weitergeleitet. Unbefugte hätten so keine Chance, von den Daten Kenntnis zu nehmen. Auf die Abfrage von Krankheits- und Urlaubstagen durch die Schulaufsicht werde aber zukünftig verzichtet, da diese Daten ohnehin von der Fachschule als personalführende Stelle erfasst würden.
Nach der Darlegung waren die so genannten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten gegen unbefugte Kenntnis nach § 9 Thüringer Datenschutzgesetz (ThürDSG) getroffen. Nicht erklärbar war jedoch, dass dem TLfDI von einem Betroffenen die ausgefüllte Liste aller Lehrer zugeleitet worden war, der nach den Einlassungen der Schulaufsicht diese Liste nicht hätte haben dürfen. Eine Befugnis eines Fachlehrers, die personenbezogenen Daten anderer Fachlehrer zur Kenntnis zu nehmen, besteht nämlich nicht. Weiterhin erhielt der TLfDI den Hinweis, ein Verfahrensverzeichnis nach § 10 ThürDSG für eine entsprechende automatisierte Datei läge nicht vor. Dabei machte die vorliegende ausgefüllte Liste eindeutig den Eindruck, dass es sich um eine automatisierte Verarbeitung der personenbezogenen Daten der Fachlehrer handelte. Der TLfDI bat die Landesanstalt daher unter Einbeziehung des behördlichen Datenschutzbeauftragten (bDSB) zu prüfen, ob eine automatisierte Datei nach § 3 Abs. 2 und 7 ThürDSG vorliege, die gemäß § 34 Abs. 2 ThürDSG hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung (auch in Papierform) der vorhe-

rigen schriftlichen Freigabe durch die verantwortliche Stelle bedürfe und in das Verfahrensverzeichnis nach § 10 ThürDSG aufzunehmen sei. Beispielsweise bietet sich in derartigen Datenverarbeitungen an, statt der Namen der Fachlehrer das Zuständigkeitsgebiet zu bezeichnen, sodass zumindest in den Fällen, in denen mehrere Lehrer dieselben Fächer unterrichten, von einer Anonymisierung nach § 3 Abs. 9 ThürDSG ausgegangen werden kann. Die Landesanstalt teilte daraufhin mit, man stimme im Ergebnis der Prüfung dem TLfDI zu, dass es sich um ein automatisiertes Verfahren handle. Die Aufnahme in das Verfahrensverzeichnis sei eingeleitet. Da einige rechtliche Einzelheiten weiterhin ungeklärt seien, sei eine datenschutzrechtliche Freigabe noch nicht erfolgt. Bis zur Freigabe habe die oberste Schulaufsichtsbehörde die Abforderung der Schuljahresanalyse jedoch ausgesetzt.
Der TLfDI wird die Angelegenheit selbstverständlich weiterhin begleiten.

Soll ein automatisiertes Verfahren zur Verarbeitung personenbezogener Daten eingesetzt werden, bedarf es der vorherigen datenschutzrechtlichen Freigabe nach § 34 Abs. 2 ThürDSG hinsichtlich der Datenarten und der regelmäßigen Datenübermittlungen. Dies bietet die Gewähr, dass die Zulässigkeit der Verarbeitung einzelner Daten nochmals hinsichtlich der Erforderlichkeit zur Aufgabenerfüllung eingehend überprüft wird. Das Verfahren ist darüber hinaus in das Verfahrensverzeichnis nach § 10 ThürDSG aufzunehmen.

6.20 Anmeldepflicht für Prostituierte?

Im Berichtszeitraum übersandte eine Nichtregierungsorganisation (NGO) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Stellungnahme den Referentenentwurf des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) für ein Gesetz zur Regulierung des Prostitutionsgewerbes sowie zum Schutz von in der Prostitution tätigen Personen.
Ziel dieses Entwurfes ist es, die Selbstbestimmung der in der Prostitution Tätigen zu schützen, ihre Arbeitsbedingungen zu verbessern und Menschenhandel zu bekämpfen. Dies soll unter anderem auch durch Meldepflichten der Betreiber von Bordellen und Prostituierten geschehen. Dabei werden auch besonders geschützte Daten im Sinne

von § 4 Abs. 5 Satz 1 Thüringer Datenschutzgesetz (ThürDSG), nämlich mit der Tatsache, dass jemand als Prostituierte oder als Prostituierter arbeitet, über das Sexualleben erhoben, verarbeitet und genutzt. Nach § 3 Abs. 1 des Entwurfs muss sich bei der zuständigen Behörde persönlich anmelden, wer eine Tätigkeit als Prostituierte oder als Prostituierter ausüben will. Damit liegt bei der jeweils zuständigen Behörde eine Liste der Personen vor, die in ihrem Bereich der Prostitution nachgehen. Der TLfDI stellte fest, dass mit dieser Tatsache oft auch eine Stigmatisierung der betroffenen Personen verbunden sein könnte und es daher nicht ausgeschlossen sei, dass sich viele betroffene Personen nicht anmelden würden, aus Angst, dass die Tatsache, dass sie der Prostitution nachgehen, bekannt wird. Zwar dürften die erhobenen Daten nach § 35 Abs. 4 Satz 1 des Gesetzentwurfs nicht an nicht-öffentliche Stellen weitergegeben werden, allerdings besteht nach § 35 Abs. 5 des Entwurfs eine Übermittlungsbefugnis an öffentliche Stellen unter den dort genannten Voraussetzungen. Insbesondere die Möglichkeit der Übermittlung, soweit die Kenntnis der Daten zur Abwehr einer gegenwärtigen Gefahr für die öffentliche Sicherheit erforderlich ist, § 35 Abs. 5 Satz 1 Nr. 2, erscheint für den TLfDI sehr weitgehend. Nicht jede Gefahr für die öffentliche Sicherheit rechtfertigt die Übermittlung derart sensibler personenbezogener Daten.
Nach Artikel 8 der Richtlinie 95/46 EG (EG-Datenschutzrichtlinie) ist die Verarbeitung personenbezogener Daten über das Sexualleben grundsätzlich untersagt. Ausnahmen sind nach Artikel 8 Abs. 4 EG-Datenschutzrichtlinie aus Gründen eines wichtigen öffentlichen Interesses möglich. Ob ein derartiges wichtiges öffentliches Interesse die Meldepflicht von Prostituierten rechtfertigt, daran bestehen hier für den TLfDI erhebliche Zweifel. Über den Ausgang des Gesetzgebungsverfahrens wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Das Verarbeiten oder Nutzen von personenbezogenen Daten über das Sexualleben (besonders geschützte Daten) ist nur zulässig, wenn die Voraussetzungen des § 4 Abs. 5 ThürDSG vorliegen. Eine solche Regelung, die dies, wie in § 4 Abs. 5 Nr. 1 ThürDSG, ausdrücklich vorsieht, muss nach Artikel 8 der Richtlinie 95/46 EG (EG-Datenschutzrichtlinie) aufgrund eines wichtigen öffentlichen Interesses jedoch geboten sein.

Rücken eines Polizisten – © Picture-Factory / Fotolia.com

7 Polizei

7.1 Aktenplanschlüssel "2124 Landfahrer": fragwürdige Sondererfassung von Sinti und Roma durch Thüringer Polizeibehörden?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Februar 2014 Post vom Zentralrat Deutscher Sinti und Roma, der auf folgenden Sachverhalt aufmerksam machte:
Der Einheitsaktenplan des Freistaats Thüringen erfasse in der Rubrik „212 Unterbringung, Besondere Personengruppen, Gefährliche Tiere“ unter dem Aktenplanschlüssel „2124 Landfahrer“ auch die Minderheit der Sinti und Roma rechtswidrig. Dieser Aktenplanschlüssel stehe ferner zwischen den weiteren Aktenplanschlüsseln „2123 Obdachlose“ und „2125 Dirnen, Bordelle“ (Prostitution). Der Zentralrat Deutscher Sinti und Roma bat den TLfDI deshalb, diese Angelegenheit zu prüfen und für die Beseitigung bzw. Löschung der diskriminierenden Akten und Dateien Sorge zu tragen.
Der TLfDI wandte sich deshalb an das damalige Thüringer Innenministerium (TIM) und wollte wissen, auf welcher Rechtsgrundlage

eine Verarbeitung von personenbezogenen Daten welcher Personen/Angehöriger nationaler Minderheiten unter dem Aktenplanschlüssel „2124 Landfahrer“ erfolge und inwieweit dies erforderlich sei.
Das TIM veranlasste daraufhin eine Prüfung in seinem Haus und im „nachgeordneten Polizeibereich“. Diese ergab, so das TIM, dass unter dem Aktenplanschlüssel „2124 Landfahrer“ keine Akten erfasst worden seien, die eine rechtswidrige Sondererfassung von Sinti und Roma beinhaltet hätten. Ferner teilte das TIM dem TLfDI mit, dass der Begriff „Landfahrer“ aus dem Einheitsaktenplan des Freistaates Thüringen gelöscht würde und die Behörden, die mit diesem Aktenplan arbeiteten, entsprechend informiert würden.
Der TLfDI war mit dieser Nachricht aus dem TIM noch nicht ganz zufrieden: Nicht beantwortet war nämlich die Frage, ob es in der Vergangenheit zu einer rechtmäßigen Sondererfassung von Sinti und Roma, die auf einer konkreten Rechtsgrundlage erfolgte, gekommen war. Die entsprechende Nachfrage des TLfDI beim TIM ergab dazu Folgendes:
Das TIM habe – nach eigener Auskunft – unter dem Aktenplanschlüssel „2124 Landfahrer“ bisher lediglich zwei Akten geführt. Diese Akten hätten aber keinen inhaltlichen Bezug zu Sinti und Roma aufgewiesen, sodass sie nunmehr dem korrekten Aktenplanschlüssel „2121 Unterbringungsrecht“ zugewiesen worden seien. Ferner teilte das TIM dem TLfDI mit, dass die Löschung des besagten Aktenplanschlüssels „2124 Landfahrer“ am 25. März 2014 erfolgt sei und der geänderte Einheitsaktenplan im Intranet unter http://www.thueringen.de/mam/th3/tim/aktenplan.pdf abgerufen werden könne. Der TLfDI teilte dieses, nicht nur datenschutzrechtlich erfreuliche Ergebnis seiner Prüfung dem Zentralrat der Sinti und Roma mit.

Die datenschutzrechtliche Prüfung des TLfDI hat mitunter zur Folge, dass Regelungen, wie der Einheitsaktenplan des Freistaates Thüringen, zwar nicht datenschutzrechtlich beanstandenswert, dafür aber sprachlich antiquiert oder misslungen sind. Wenn dann die Behörde auf den Hinweis des TLfDI entsprechend reagiert und das Regelwerk umgehend ändert und „verbessert“, hat die Arbeit des TLfDI einen willkommenen „Nebeneffekt“, nämlich, dass Normen und Paragra-

fen für den Bürger leicht verständlich und nicht diskreditierend formuliert sind.

7.2 Interessenkollisionen beim Polizeiärztlichen Dienst

Von der Landesärztekammer Thüringen erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den Hinweis auf datenschutzrechtliche Probleme beim PÄD (= polizeiärztlicher Dienst) der Thüringer Polizei.
Die Polizeiärzte haben verschiedene Funktionen und Bereiche abzudecken. Zum einen ist dies die Sicherstellung der arbeitsmedizinischen Betreuung auf der Grundlage des Arbeitssicherheitsgesetzes (ASiG) in allen Behörden, Einrichtungen und Dienststellen der Thüringer Polizei. Weiterhin müssen Untersuchungen bezüglich Fragen der gesundheitlichen Eignung bei allgemeinen personalrechtlichen Entscheidungen durchgeführt werden. Darüber hinaus besteht die Aufgabe, die ärztliche Versorgung und medizinische Betreuung der heilfürsorgeberechtigten Polizeivollzugsbeamten nach den Heilfürsorgebestimmungen wahrzunehmen. Hinzu kommt die Sicherstellung der medizinischen Betreuung und der psychologischen Beratung und Betreuung im Rahmen von Einsätzen, Übungen und Ausbildungsmaßnahmen. Dabei unterscheiden sich die Aufgaben teilweise wesentlich in Zweckrichtung und Interessenssphäre.
Problematisch wird diese Aufgabenvielfalt dann, wenn mehrere dieser Bereiche von einem einzelnen Arzt wahrgenommen werden. Wird der Polizeiarzt im Rahmen der Heilfürsorge oder Arbeitsmedizin tätig, unterliegt er auch gegenüber dem Dienstherrn der ärztlichen Schweigepflicht. Für allgemeine beamtenrechtliche Entscheidungen dürfen diese Daten daher nur mit ausdrücklicher Einwilligung des Betroffenen weiterverarbeitet werden, es sei denn, es liegt eine gesetzliche Offenbarungsbefugnis oder Offenbarungspflicht vor. Muss derselbe Polizeiarzt aber auch Untersuchungen für personalrechtliche Entscheidungen durchführen, besteht die Gefahr einer Interessenskollision und einer möglichen bewussten oder unbewussten Beeinflussung von Personalentscheidungen durch die Kenntnis von heilfürsorge- bzw. arbeitsmedizinischen Daten.
Um dies zu vermeiden, bedarf es einer notwendigen räumlichen, organisatorischen und gegebenenfalls auch personellen Trennung für die Gewährleistung der Einhaltung der ärztlichen Schweigepflicht.

Insbesondere müssen die Bereiche der Heilfürsorge und der Betriebsmedizin von der amtsärztlichen Begutachtung getrennt sein.
Auf Anfrage zu diesen Interessenskonflikten hat das Thüringer Ministerium für Inneres und Kommunales (TMIK) zunächst mitgeteilt, bislang seien die mit betriebsärztlichen Aufgaben befassten Mediziner im polizeiärztlichen Dienst auch mit Amts- und anderen polizeiärztlichen Aufgaben betraut. Es sei beabsichtigt, künftig die Trennung von betriebs- und amtsärztlichen Aufgaben vorzusehen. Der bereits bestellte sowie ein noch zu bestellender Betriebsmediziner der Thüringer Polizei würden danach ausschließlich die Aufgaben nach § 3 des Gesetzes über Betriebsärzte, Sicherheit und andere Fachrichtungen für Arbeitssicherheit (ASiG) wahrnehmen.
Dies war aber noch keine umfassende Lösung zu dem dargestellten Interessenkonflikt. Auf Nachhaken hat das TMIK ergänzend erläutert, dass die für den polizeiärztlichen Dienst verbleibenden Bereiche der Behandlung von Anwärtern im Rahmen der Heilfürsorge und der Durchführung von Untersuchungen zur Unterstützung personalrechtlicher Entscheidungen aufgrund der vorhandenen Personalkapazitäten nicht strikt und vollständig getrennt werden könnten. Die Einstellung weiterer Ärzte sei aufgrund der haushaltsrechtlichen Vorgaben nicht zu realisieren. Die beiden Bereiche seien jedoch rechtlich, funktional und organisatorisch getrennt. Der Bereich der Heilfürsorge sei vor allem in Meiningen angesiedelt. Die beamtenrechtlichen Untersuchungen würden in der Regel durch den Leiter des Polizeiärztlichen Dienstes durchgeführt, weil er grundsätzlich keine Behandlung im Rahmen der Heilfürsorge wahrnehme. Sollte ausnahmsweise ein Arzt, der einen Beamten bereits im Rahmen der Heilfürsorge betreut hat, mit der Durchführung der beamtenrechtlichen Untersuchung betraut werden, so behalte sich der Leiter des PÄD bei dem Verdacht dessen möglicher Beeinflussung aus der Zeit der Heilfürsorge die eigene Bearbeitung der Vorgänge jederzeit vor. Damit wurde das Problem bis auf wenige Einzelfälle gelöst.
Inzwischen hat der TLfDI allerdings erfahren, dass man als zweiten Betriebsmediziner nicht etwa einen zusätzlichen Arzt eingestellt, sondern einen bereits im Polizeiärztlichen Dienst tätigen Arzt bestellt hatte. Auf diese Weise ergibt sich zwar eine Entspannung des betriebsmedizinischen Dienstes, die übrigen Aufgaben konzentrieren sich aber auf eine Person weniger. Ob damit den Festlegungen nachgekommen werden kann, wird vom TLfDI weiterhin überprüft.

Es ist immer problematisch, wenn ein und derselbe Arzt verschiedene Aufgaben wahrnehmen muss, aber die Erkenntnisse aus der einen Tätigkeit nicht für die andere Tätigkeit nutzen darf. Um Interessenskollisionen zu vermeiden, sollte am besten immer eine strikte personelle Trennung eingehalten werden.

7.3 NSU-Untersuchungsausschuss des Thüringer Landtags – Beweise vs. Datenschutz

Das ehemalige Thüringer Innenministerium (nunmehr Thüringer Ministerium für Inneres und Kommunales) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum, eine datenschutzrechtliche Einschätzung gemäß § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hinsichtlich der Vorlage von Personalakten im Rahmen des Untersuchungsausschusses (UA 5/1) des Thüringer Landtags „Rechtsterrorismus und Behördenhandeln“ abzugeben.
Nach einem dem UA 5/1 vorliegenden Beweisantrag sollten dem Ausschuss alle in einem bestimmten Zeitraum zur Personalakte genommenen Vorgänge, insbesondere Stellenbeschreibungen, Versetzungen, einschließlich Gesuche, Anordnungen, zeitweilige Sonderaufgaben, dienstliche Äußerungen, dienstliche Weisungen, Disziplinarmaßnahmen, Beurteilungen, Beförderungsempfehlungen und -anträge sowie Fehlzeiten von Bediensteten zweier Ermittlungsgruppen vorgelegt werden und es sollte schriftlich darüber Auskunft erteilt werden, welche der zuvor beschriebenen Akten, Aktenbestandteile und Dokumente sowie darin enthaltenen Daten seit 1995 vernichtet bzw. gelöscht und welche Akten, Aktenbestandteile und Dokumente im Original bzw. in Kopie an dritte Stellen abgegeben wurden.
Nach § 14 Abs. 1 Thüringer Untersuchungsausschussgesetz (UAG) ist unter anderem die Landesregierung verpflichtet, die vom Untersuchungsausschuss angeforderten Akten vorzulegen und Auskünfte zu geben.
Der TLfDI stellte, wie zuvor bereits schon am Anfang der Jahre 2012 und 2013 fest, dass nach § 14 Abs. 3 UAG die Verpflichtung zur Vorlage nicht besteht, wenn insbesondere nach § 14 Abs. 3 Nr. 3 UAG in Grundrechte eingegriffen würde. Die Berufung auf die Gründe in § 14 Abs. 3 Nr. 3 UAG ist jedoch ausgeschlossen, soweit der unantastbare Bereich privater Lebensgestaltung nicht betroffen

und der Grundsatz der Verhältnismäßigkeit beachtet ist (§ 14 Abs. 3 Satz 2, 2. Alt. UAG). Im Hinblick auf die in dem Beweisbeschluss angeforderten Personalakten musste der TLfDI grundsätzlich davon ausgehen, dass diese personenbezogene Daten enthielten.
Unter Berücksichtigung der Rechtsprechung, insbesondere des Beschlusses des Bundesverfassungsgerichts (Beschluss BVerfG 2 BvE 3/07, zitiert nach juris, Rz. 113) muss bei einem Ersuchen auf Aktenvorlage nicht bereits feststehen, dass die Unterlagen auch tatsächlich entscheidungserhebliches Material oder entsprechende Beweismittel enthalten. Es reicht bereits aus, wenn die Unterlagen Hinweise geben könnten.
Die Landesregierung legt – soweit sie Ausschlussgründe annimmt – dem Untersuchungsausschuss nach § 14 Abs. 4 UAG die Gründe einer Verweigerung in nicht-öffentlicher, gegebenenfalls vertraulicher Sitzung dar. Hält der Untersuchungsausschuss die Voraussetzungen der Verweigerung nicht für gegeben, kann er mit der Mehrheit seiner Mitglieder beschließen, den Verfassungsgerichtshof anzurufen. Der Verfassungsgerichtshof entscheidet nach Maßgabe des Gesetzes über den Thüringer Verfassungsgerichtshof (ThürVerfGHG) darüber, ob die Verweigerung begründet ist; erklärt er die Verweigerung für unbegründet, darf sie nicht aufrechterhalten werden.
Im Falle einer Vorlageverweigerung des Thüringer Innenministeriums hinsichtlich der Personalunterlagen, die ersichtlich für die Aufgabenerfüllung des Untersuchungsausschusses nicht erforderlich sind, war für den konkreten Fall in der Abwägung der Grundsatz der Verhältnismäßigkeit einzubeziehen. So war hier nicht auszuschließen, dass beispielsweise personenbezogene Daten Dritter in den hier gegenständlichen Personalakten hätten enthalten sein können, die keinen Bezug zum Untersuchungsgegenstand hatten. Die Abwägung zwischen der verfassungsrechtlichen Stellung des Untersuchungsausschusses und dem Eingriff in das Grundrecht auf informationelle Selbstbestimmung eines in der Regel völlig unbeteiligten Dritten musste dabei nach der Auffassung des TLfDI grundsätzlich zugunsten des betroffenen Dritten ausfallen. Im Rahmen der Abwägung zwischen dem Aufklärungsinteresse des Untersuchungsausschusses und den berechtigten und grundrechtlichen geschützten Interessen der betroffenen Personen war jedoch beispielsweise auch die Möglichkeit einer partiellen Schwärzung von personenbezogenen Daten in Betracht zu ziehen.

Der Untersuchungsausschuss erhebt gemäß § 13 UAG die durch den Untersuchungsauftrag gebotenen Beweise aufgrund von Beweisbeschlüssen. In den Beweisbeschlüssen müssen die Tatsachen, über die Beweis erhoben werden soll, und die Beweismittel bezeichnet werden.
Die Landesregierung und die Behörden des Landes sowie die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen, sind gemäß § 14 UAG verpflichtet, die von dem Untersuchungsausschuss angeforderten Akten vorzulegen und Auskünfte zu geben, Zutritt zu den von ihnen verwalteten öffentlichen Einrichtungen zu gewähren sowie die erforderlichen Aussagegenehmigungen zu erteilen. Die Verpflichtung besteht gemäß § 14 Abs. 3 UAG grundsätzlich nicht, wenn durch deren Erfüllung interne Beratungen und Entscheidungen offenbart würden, die zum unausforschbaren Kernbereich der exekutiven Eigenverantwortung gehören, dem Wohle des Landes, des Bundes oder eines anderen deutschen Landes Nachteile bereitet würden oder in Grundrechte eingegriffen würde. Dies ist im Einzelfall zu prüfen.

7.4 Klick und Blick – mit erheblichen Konsequenzen! – INPOL-Abfrage nur bei Erforderlichkeit

Ein Beschwerdeführer wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und schilderte im Rahmen eines persönlichen Gespräches, dass eine dritte Person ihn auf seine vermeintlichen Vorstrafen ansprach. Verwundert über die Herkunft dieser Informationen, bat der Beschwerdeführer den TLfDI um Hilfe.
Der TLfDI wandte sich sogleich an die Landespolizeidirektion in Erfurt und bat zur Aufklärung dieses Sachverhaltes um eine Stellungnahme. Zur Prüfung des Sachverhaltes war es wichtig, zu wissen, ob die Polizei die personenbezogenen Daten zu dem Beschwerdeführer abfragte, wann dies geschah und auf welcher Rechtsgrundlage eine mögliche Datenabfrage erfolgte.
In ihrer Stellungnahme teilte die Landespolizeidirektion mit, dass aufgrund einer durch das Thüringer Landeskriminalamt durchgeführten Protokollrecherche ein Angehöriger der Thüringer Polizei tatsächlich im IT-System INPOL unberechtigt – also ohne dienstlichen Auftrag – eine Abfrage zu dem Namen des Beschwerdeführers getä-

tigt hatte. Welche konkreten Erkenntnisse der Angehörige der Thüringer Polizei im Rahmen dieser Abfrage erlangte, war jedoch nicht mehr nachvollziehbar, da die Aussonderungsprüffrist (Homepage TLfDI: Leitfaden über die Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut) für die personenbezogenen Daten des Beschwerdeführers bereits abgelaufen war. Damit waren sämtliche personenbezogene Daten des Beschwerdeführers im INPOL-System gelöscht.
Grundsätzlich ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift (beispielsweise das Polizeiaufgabengesetz oder die Strafprozessordnung) sie erlauben oder der Betroffene einwilligt. Da in diesem Sachverhalt für die Abfrage kein dienstlicher Auftrag zugrunde lag, erfolgte diese rechtsgrundlos und damit unberechtigt.
Diese datenschutzrechtliche Verletzung hat der TLfDI gemäß § 39 Abs.1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet. Ein Ermittlungsverfahren gegen den Angehörigen der Thüringer Polizei leitete die Landespolizeidirektion ein.
Der TLfDI wies die Landespolizeidirektion darauf hin, dass seitens der zuständigen Stellen darauf zu achten ist, dass entsprechende Abfragen nur im gesetzlich erforderlichen und tatsächlich benötigten Maß vorzunehmen sind. Zur Umsetzung dieser Maßnahmen teilte die Landespolizeidirektion mit, dass die Angehörigen der Thüringer Polizei halbjährlich darüber belehrt würden. Zudem sei die Dienstanweisung zur Einhaltung datenschutzrechtlicher Bestimmungen in der Landespolizeidirektion bei der jährlichen Belehrung Gegenstand. Unabhängig davon sensibilisiere und belehre der behördliche Datenschutzbeauftragte die Mitarbeiter nochmals schriftlich hinsichtlich der Unzulässigkeit unbefugter Datenabfragen.
Der TLfDI begrüßt diese Maßnahmen und hofft auf eine strikte Einhaltung.

Es mag verlockend sein, mit wenigen Klicks Einblicke in die Persönlichkeit eines Dritten zu erlangen. Insbesondere dann, wenn man als Angehöriger der Polizei die Möglichkeit hat, polizeiliche Auskunfts- und Recherchesysteme zu nutzen. Eine unerlaubte Abfrage hat jedoch erhebliche Konsequenzen: Nicht nur, dass der TLfDI dies gemäß § 39 ThürDSG beanstandet, sondern auch, dass diese Abfragen

eine Ordnungswidrigkeit oder im schlimmsten Fall eine Straftat nach § 43 ThürDSG darstellen können.

7.5 Rasterfahndungen in Thüringen – nicht ohne TLfDI

Bei verschiedenen polizeilichen Maßnahmen ist auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einzubeziehen, so zum Beispiel, wenn die Sicherheitsbehörden eine Rasterfahndung durchführen. Die Rasterfahndung ist ein automatisierter Datenabgleich, bei dem bestimmte Merkmale, die auf den Täter oder die gesuchte Person zutreffen könnten, mit entsprechenden Daten, die bei verschiedenen anderen Stellen vorhanden sind, abgeglichen werden. Damit sollen zum einem unverdächtige Personen ausgeschlossen und zum anderen Personengruppen, die als mögliche Täter in Betracht kommen, eingegrenzt werden. Im Gegensatz zu den gewöhnlichen Ermittlungen existiert bei einer Rasterfahndung gerade noch keine konkrete Zielperson. Bei der Rasterfahndung handelt es sich um einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes [GG], Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen [ThürVerf]).

Bei einem Einsatz der Rasterfahndung im Rahmen der Strafverfolgung nach § 98a Strafprozessordnung (StPO) ist gemäß § 98b Abs. 4 StPO nach Beendigung dieser durchgeführten Maßnahme die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist. Wird die Rasterfahndung im Rahmen der Gefahrenabwehr eingesetzt, so richtet sich ihre Rechtmäßigkeit nach § 44 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (PAG). § 44 in Absatz 4 PAG bestimmt, dass von der Maßnahme der TLfDI unverzüglich zu unterrichten ist.

Da sich die Unterrichtungspflicht relativ gut in den entsprechenden Normen „versteckt“, nahm der TLfDI im Rahmen seiner Kontrollbefugnis gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) dies zum Anlass, einmal nachzufragen, wie viele Rasterfahndungen die Thüringer Sicherheitsbehörden sowohl im strafprozessualen als auch im präventiven Bereich in Thüringen seit dem Jahr 2009 angeordnet und durchgeführt hatten und ob jeweils eine Unterrichtung an den TLfDI erfolgte. Das Ergebnis war aus datenschutzrechtlicher Sicht sehr erfreulich. Im Abfragezeitraum erfolgte weder zu strafprozessu-

alen noch zu präventiven polizeilichen Zwecken eine Rasterfahndung. Eine Unterrichtung des TLfDI war deshalb nicht nötig.

Besonders bei polizeilichen Maßnahmen weiß der Bürger oft nicht, was mit seinen personenbezogenen Daten geschieht. Das Grundrecht auf informationelle Selbstbestimmung beinhaltet jedoch die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 149, zitiert nach juris). Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig (BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 150, 151, zitiert nach juris). Greift der Staat in das Grundrecht auf informationelle Selbstbestimmung, welches Bestandteil des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 6 Abs. 2 ThürVerf) ist, ein, bedarf dies daher einer klaren gesetzlichen Grundlage. Diese gesetzlichen Grundlagen sind insbesondere in der Strafprozessordnung und im Polizeiaufgabengesetz festgelegt. Nur unter den dort genannten Voraussetzungen ist ein Eingriff in das Grundrecht zulässig. Bei einer Rasterfahndung ist der TLfDI zu unterrichten.

7.6 Unerlaubt und daher beanstandet – Abfrage personenbezogener Daten durch die Polizei

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er seine schutzwürdigen Belange bei der Verarbeitung und Nutzung seiner personenbezogenen Daten in einem gegen ihn geführten strafrechtlichen Ermittlungsverfahren beeinträchtigt sah.
Hintergrund war, dass die Polizei zu dem Betroffenen eine SARS-Abfrage durchgeführt hatte. Die Rechtmäßigkeit dieser Maßnahme zweifelte der Beschwerdeführer an.
Das SYBORG Auskunfts- und Recherche-System – kurz SARS – ist ein automatisiertes Verfahren, um zum Zweck der Gefahrenabwehr und im Zuge der Verfolgung von Straftaten Informationen über den Inhaber einer Rufnummer ermitteln zu können.
Rechtsgrundlagen für eine SARS-Abfrage sind die §§ 161, 163 Strafprozessordnung (StPO) – Ermittlungsgeneralklau-

seln – in Verbindung mit § 112 Telekommunikationsgesetz (TKG). Nach § 112 Abs. 2 Nr. 1 TKG werden Auskünfte aus den Kundendateien der Telekommunikationsunternehmen den Strafverfolgungsbehörden jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Strafverfolgungsbehörden ihre Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorlegen. Die Bundesnetzagentur hat die entsprechenden Datensätze aus den Kundendateien abzurufen und an die ersuchende Stelle zu übermitteln.

Die Auskünfte dürfen die Telekommunikationsunternehmen nur erteilen, sofern sie für die Aufgabenwahrnehmung der ersuchenden Strafverfolgungsunternehmen erforderlich sind. Dies stellt sicher, dass Abfragen nicht leichthändig zur bloß orientierenden Vorabinformation getätigt werden, sondern nur dann, wenn die Behörde die von ihr zur Aufgabenwahrnehmung tatsächlich benötigten Informationen nicht auf andere Weise einfacher, aber ebenso effektiv beschaffen kann (BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, Rn. 157).

Im konkreten Fall fand sich in der Ermittlungsakte selbst jedoch kein weiterer Hinweis darauf, dass die abgefragten Telefonnummern tatsächlich für die weiteren Ermittlungen genutzt werden sollten. Der TLfDI musste daher anhand der Ermittlungsunterlagen davon ausgehen, dass die konkrete SARS-Abfrage nicht erforderlich gewesen war. Der gegen den Betroffenen erhobene Vorwurf stützte sich lediglich auf Vermutungen und vage Anhaltspunkte. Zum Zeitpunkt der Abfrage war noch nicht einmal hinreichend geklärt, ob es überhaupt einen Täter gab. Die getätigte SARS-Abfrage stand aus Sicht des TLfDI daher nicht im angemessenen Verhältnis zur Stärke des Tatverdachts gegen den Beschwerdeführer. Es kamen zudem neben dem Betroffenen auch weitere Personen als mögliche Verdächtige in Betracht. Doch lediglich bei dem betroffenen Beschwerdeführer fand eine SARS-Abfrage statt. Dass die abfragende Behörde diese Daten tatsächlich benötigte, war für den TLfDI nicht erkennbar. Vielmehr lag es in diesem Sachverhalt nahe, dass sie die SARS-Auskunft zur bloßen Vorabinformation begehrte, was jedoch von der Rechtsgrundlage des § 112 Abs. 2 Nr. 1 TKG nicht gedeckt ist.

Diese datenschutzrechtliche Verletzung hat der TLfDI gemäß § 39 Abs. 1 Thüringer Datenschutzgesetz beanstandet.

Der Polizei steht bei der Erforschung und Ermittlung des Sachverhaltes eine Reihe von Instrumenten zur Verfügung, die oft nicht nur unwesentlich in das Recht auf informationelle Selbstbestimmung der Betroffenen eingreifen. In dem hier geschilderten Fall musste die auf die Ermittlungsgeneralklausel gestützte Maßnahme jedoch zur Aufgabenerfüllung erforderlich sein. Ist sie es nicht, wie in diesem Fall, hätte von der Maßnahme Abstand genommen werden müssen. Eine Aufklärung um jeden Preis ist durch den Gesetzgeber gerade nicht vorgesehen.

7.7 Verwechslung beim Strafbefehl

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und informierte darüber, dass er einen Strafbefehl erhalten habe, in dem er einer Straftat beschuldigt wurde. Der Strafbefehl enthielt zudem die Angabe eines Geburtsdatums sowie eines Geburtsortes, welche jedoch nicht der Person des Beschwerdeführers zugeordnet werden konnten. Offensichtlich handelte es sich hier um eine Verwechslung. Der Beschwerdeführer legte gegen diesen Strafbefehl Einspruch ein.
Der TLfDI fragte beim zuständigen Gericht nach, wie es dazu kommen konnte, dass es den Strafbefehl nicht an den eigentlichen Beschuldigten, sondern an eine andere Person – den Beschwerdeführer – übermittelte, woher die Daten des Beschwerdeführers stammten und ob die personenbezogenen Daten des Beschwerdeführers zwischenzeitlich gelöscht wurden. Das zuständige Gericht konnte diese Fragen nicht abschließend beantworten und verwies den TLfDI an die Staatsanwaltschaft zur weiteren Sachverhaltsaufklärung.
Auf Nachfrage des TLfDI teilte die Staatsanwaltschaft mit, dass sie aus der Ermittlungsakte nicht mehr nachvollziehen konnte, wie die bis zum Abschluss des Ermittlungsverfahrens korrekt erfassten Daten geändert wurden. Nachdem die Staatsanwaltschaft den Fehler infolge des Einspruchs des Beschwerdeführers bemerkt hatte, nahm sie den Strafbefehl zurück. Dies teilte die Staatsanwaltschaft dem Beschwerdeführer auch mit. Gleichzeitig bot das zuständige Gericht dem Beschwerdeführer Hilfe bei der Beseitigung von Nachteilen an, die durch das fehlerhaft gegen ihn geführte Strafbefehlsverfahren möglicherweise entstanden waren.

Darüber hinaus konnte der TLfDI erreichen, dass die personenbezogenen Daten des Beschwerdeführers sowohl aus der Vorgangsbearbeitungsdatei des Gerichtes als auch in dem Datenverarbeitungssystem der Staatsanwaltschaft gelöscht wurden.
Da es sich bei diesem Fall um ein Versehen handelte und die zuständigen Stellen die personenbezogenen Daten des Beschwerdeführers gelöscht hatten, sah der TLfDI von einer Beanstandung ab.

Fügt eine Daten verarbeitende Stelle einem Betroffenen durch eine nach dem Thüringer Datenschutzgesetz (ThürDSG) oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen gegenüber gemäß § 18 ThürDSG grundsätzlich zum Ersatz dieses Schadens verpflichtet. Die Ersatzpflicht entfällt, soweit die nach den Umständen des Falls gebotene Sorgfalt beachtet wurde. Den Schadensersatzanspruch muss der Betroffene selbst geltend machen, der TLfDI kann dies nicht für den Betroffenen übernehmen. Sofern der Rechtsweg beschritten werden muss, steht dieser zu den ordentlichen Gerichten offen.

7.8 Bei rechtmäßiger Wohnungsdurchsuchung kann auch der TLfDI nicht mehr helfen

Im Berichtszeitraum wandte sich eine Beschwerdeführerin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um dessen Hilfe.
Sie teilte mit, dass eine Hausdurchsuchung bei ihr stattgefunden hätte und die Beamten dabei diverse Gegenstände (Computer, Handy) beschlagnahmt hätten. Sie sah sich in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt.
Daraufhin fragte der TLfDI bei der zuständigen Staatsanwaltschaft nach, auf welcher Rechtsgrundlage die Durchsuchung und die Beschlagnahme bei der Beschwerdeführerin stattgefunden hätten. Zudem nahm der TLfDI Einsicht in die staatsanwaltschaftliche Ermittlungsakte. Darin befand sich ein richterlicher Durchsuchungs- und Beschlagnahmebeschluss. Liegt ein solcher richterlicher Durchsuchungs- und Beschlagnahmebeschluss vor, ist er für die Strafverfolgungsbehörden in seiner Umgrenzungsfunktion maßgeblich. Er konkretisiert die Durchsuchungs- und Beschlagnahmenormen der §§ 94, 98, 102, 105 Strafprozessordnung (StPO). Anhaltspunkte

dafür, dass die Polizeibeamten während der Durchführung der Durchsuchung außerhalb dieses Beschlusses handelten, ergaben sich aus der Ermittlungsakte nicht. Ein datenschutzrechtlicher Verstoß lag somit auch nicht vor.
Eine Überprüfung des richterlichen Beschlusses (d. h., ob dieser inhaltlich so hätte erlassen werden dürfen) war mangels Zuständigkeit des TLfDI nicht möglich. Nach § 2 Abs. 6 Thüringer Datenschutzgesetz gilt der Fünfte Abschnitt (u. a. die Kontrolle [§ 37], die Unterstützungspflicht [§ 38] und die Beanstandung [§ 39]) für Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Der richterliche Durchsuchungs- und Beschlagnahmebeschluss stellte indes keine Verwaltungsangelegenheit dar, sondern war im Rahmen der richterlichen Unabhängigkeit erlassen worden.
Für die Beschwerdeführerin bestand die Möglichkeit, Beschwerde gegen den Beschluss des Amtsgerichts einzulegen.

Nach § 37 Thüringer Datenschutzgesetz kontrolliert der TLfDI bei allen öffentlichen Stellen die Einhaltung der Bestimmungen dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz. In bestimmten Fällen ist die Kontrolle des TLfDI beschränkt. Das gilt zum Beispiel für die Gerichte. Grund hierfür ist die verfassungsrechtlich garantierte richterliche Unabhängigkeit gemäß Art. 86 Abs. 2 der Verfassung des Freistaats Thüringen.

7.9 Datenabfrage oder keine Datenabfrage – das ist hier die Frage

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte seine Befürchtung mit, dass eine Person einer konkreten Thüringer Polizeidienststelle möglicherweise über die der Thüringer Polizei zur Verfügung gestellten Daten der Einwohner- und Meldeämter eine Abfrage zu seiner Adresse durchgeführt habe. Nach Ansicht des Beschwerdeführers hatte er seine Adresse niemandem mitgeteilt. Der TLfDI wies den Beschwerdeführer zunächst darauf hin, dass, unabhängig von einer Recherche in den polizeilichen Informationssystemen, auch eine Auskunft zu seiner Anschrift nach § 31 Thüringer Meldegesetz (ThürMeldeG) möglich ist. Danach darf die Meldebehörde Personen, die nicht Betroffene sind, und anderen als den in § 28 Abs. 1 ThürMeldeG bezeichneten

Stellen Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner erteilen (einfache Melderegisterauskunft). Insofern war es in diesem Fall nicht auszuschließen, dass jemand eine derartige Auskunft auch direkt beim Meldeamt beantragt hatte und diese ihm erteilt wurde. Der Beschwerdeführer glaubte jedoch, dass die Datenabfrage von einem Angehörigen der Polizei vorgenommen wurde. Deshalb bat der TLfDI die zuständige Polizeiinspektion um eine Stellungnahme, ob ein Bediensteter dieser Stelle die Personalien des Beschwerdeführers abgefragt habe und auf welcher Rechtsgrundlage dies geschehen sei. Die Polizeiinspektion gab den Sachverhalt zuständigkeitshalber an die Landespolizeidirektion ab, um dort eine Prüfung zu veranlassen. Im Ergebnis teilte die Landespolizeidirektion mit, dass kein Angehöriger der Polizeiinspektion in den durch die Einwohner- und Meldeämter zur Verfügung gestellten Daten bzw. in den Datensätzen des Kraftfahrt-Bundesamtes (Zentrales Verkehrsinformationssystem (ZEVIS)) Abfragen zu der Person des Beschwerdeführers durchgeführt habe. Auch eine nochmalige Nachfrage des TLfDI, ob eine konkret benannte Person Abfragen in den polizeilichen Auskunftssystemen vorgenommen habe, ergab, dass dies nicht der Fall war.
Einen möglichen datenschutzrechtlichen Verstoß konnte der TLfDI damit nicht nachweisen.

Für eine Datenabfrage kann außerhalb des Polizeibereiches als Rechtsgrundlage beispielsweise auch § 31 ThürMeldeG in Betracht kommen. Diese Vorschrift regelt die einfache Melderegisterauskunft. § 32 ThürMeldeG sieht unter den dort genannten Voraussetzungen die Melderegisterauskunft in besonderen Fällen für Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen vor.
Seit dem 1. November 2015 gilt nunmehr das Bundesmeldegesetz, welches für das gesamte Bundesgebiet einheitliche und unmittelbar geltende Vorschriften für die Bürger auch zur Melderegisterauskunft normiert.

7.10 Drehort Hörsaal – und Action! – Videogaga 3 – Aufzeichnung einer Dienstversammlung

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte Kenntnis darüber, dass bei einer

vergangenen Dienstversammlung im Hörsaal des Bildungszentrums der Thüringer Polizei in Meiningen (BZ Meiningen), zu deren Teilnahme die Bediensteten verpflichtet waren, zwei Videokameras die Bediensteten ohne deren Kenntnis und ohne deren Einwilligung aufgezeichnet hatten.

Bei der eingesetzten Videotechnik handelte es sich zum einen um eine Stativkamera und zum anderen um die in dem Hörsaal fest installierte Deckenkamera. Beide Kameras zeichneten die ca. zweistündige Dienstversammlung in Bild und Ton komplett auf. Dabei wusste insbesondere einer der auf der Bühne befindlichen Redner nicht, dass er aufgenommen wurde. Im Aufnahmebereich waren zudem ca. fünf bis sieben Personen von hinten zu sehen. Auch die Fragen der Teilnehmer an die Redner zeichneten die Videokameras auf. Über die Videoaufnahmen in Bild und Ton hatten die Verantwortlichen des BZs Meiningen die anwesenden Bediensteten vorab weder informiert, noch hatten Letztere eingewilligt, Videoaufnahmen von sich fertigen zu lassen.

Als Rechtfertigung für die Aufnahmen führte das Bildungszentrum an, dass diese Aufzeichnungen für Protokollzwecke gefertigt worden seien und man es vergessen habe, die Bediensteten vor Beginn der Veranstaltung darauf hinzuweisen. Dies sei ein Versehen gewesen.

Nach § 4 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Eine spezialgesetzliche Rechtsvorschrift lag in diesem Fall nicht vor, sodass die Videoaufnahmen nur aufgrund einer Einwilligung der Betroffenen möglich gewesen wären. Eine Einwilligung ist gemäß § 4 Abs. 2 ThürDSG die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen.

Die Einwilligung muss der Verarbeitung vorausgehen (Simitis in: Bundesdatenschutzgesetz, Kommentar, § 4a, Rn. 27). Damit soll unter anderem vermieden werden, dass die Betroffenen vor vollendete Tatsachen gestellt werden, weil es oft kaum noch einen Sinn hat, sich gegen eine bereits erfolgte Datenverarbeitung zu wehren (Simitis, a.a.O.). Deshalb stellt beispielsweise auch eine nachträgliche Genehmigung ebenfalls keine Einwilligung dar, und eine Heilung eines solchen Mangels sieht das ThürDSG ebenfalls nicht vor.

Im vorliegenden Sachverhalt setzten die Verantwortlichen des BZ Meiningen die Betroffenen erst am Ende der Veranstaltung und nur aufgrund der ausdrücklichen Nachfrage eines Bediensteten, ob diese Veranstaltung aufgezeichnet werde, in Kenntnis über die Videoaufnahmen. Der vom BZ Meiningen vertretenen Ansicht, dass von einem Einverständnis der Betroffenen ausgegangen werden könnte, da nach dem Hinweis des Bediensteten die Betroffenen keine Einwände gegen die Aufzeichnungen erhoben hatten, konnte sich der TLfDI aus den oben genannten Gründen nicht anschließen.
Das Aufzeichnen der Dienstversammlung mittels zweier Videokameras ohne Rechtsgrundlage und ohne die Einwilligung der Betroffenen verstieß gegen § 4 Abs. 1, 2 und 3 ThürDSG. Der TLfDI beanstandete dies gemäß § 39 Abs. 1 ThürDSG.
Im Nachgang teilte das BZ Meiningen mit, dass es als erste Konsequenz aus der Beanstandung die Deckenkamera umgehend außer Betrieb gesetzt habe. Des Weiteren drehten die Verantwortlichen des BZ Meiningen das Objektiv der Kamera in Richtung Raumdecke, sodass eine Aufnahme der Bühne bzw. des Plenums nicht mehr erfolgen konnte. Sofern die Notwendigkeit einer Nutzung der Bild- und Tontechnik in Form von Aufzeichnungen von Veranstaltungen in diesem Hörsaal besteht, will das BZ Meiningen künftig im Vorfeld von allen Beteiligten eine entsprechende Einwilligungserklärung im Sinne des § 4 Abs. 2, 3 ThürDSG einholen. Zudem wird das BZ Meiningen eine geplante Aufzeichnung zukünftig ausdrücklich kommunizieren. Der TLfDI begrüßte diese Maßnahmen.

Wird die Einwilligung bei dem Betroffenen eingeholt, ist er nach § 4 Abs. 3 ThürDSG auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur (§ 2 Nr. 3 des Signaturgesetzes vom 16. Mai 2001 BGBl. I S. 876 – in der jeweils geltenden Fassung), soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

7.11 Prüf- und Löschfristen der Polizei – Fortsetzung folgt ...

Ein Beschwerdeführer, der sich bereits im Jahr 2012 an den TLfDI gewandt und um die Prüfung der Zulässigkeit der Speicherung seiner Daten gebeten hatte (siehe hierzu 10. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Punkt 7.8) rief Anfang des Jahres 2015 erneut den TLfDI an und bat darum, die nach seiner Auffassung rechtwidrigen Einträge in den polizeilichen Datenbanken zu löschen.
Der TLfDI prüfte den Fall und musste dem Beschwerdeführer jedoch mittteilen, dass sich die Rechtslage hinsichtlich der Speicherung seiner Daten seit dem Jahr 2012 nicht geändert hatte. Das Prüfergebnis, das der TLfDI dem Beschwerdeführer Ende 2012 mitgeteilt hatte, hatte noch immer Bestand. Insofern konnte der TLfDI aus datenschutzrechtlicher Sicht keine Löschung seiner Daten fordern, da ihre Speicherung noch immer rechtmäßig war.
Gemäß § 40 Abs. 2 Satz 1 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (PAG) in Verbindung mit § 2 Abs. 1 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) beträgt die Prüffrist zur Löschung der Daten bei Erwachsenen und Jugendlichen fünf Jahre. Dabei beginnt diese Aussonderungsprüffrist gemäß § 40 Abs. 2 Satz 4 PAG i. V. m. § 5 ThürPolPrüffristVO grundsätzlich mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat. Sofern sich die laufenden Verfahren beim Beschwerdeführer erledigen und er nicht erneut polizeilich in Erscheinung tritt, werden die Daten des Beschwerdeführers aus dem Jahr 2012 mit Ablauf der Aussonderungsprüffrist im Jahr 2017 aus dem polizeilichen Informationssystem gelöscht.
Die Nachfrage an den Beschwerdeführer, ob gegebenenfalls neue Sachverhalte vorlägen, welche einen anderen Fristablauf zur Folge hätten, blieb ergebnislos. Der TLfDI sah damit den Fall als erledigt an.

§ 5 Abs. 1 Satz 1 ThürPolPrüffristVO gilt als „Jungbrunnen“ bei Prüf- und Löschfristen personenbezogener Daten, die die Polizei speichert. Soweit innerhalb der Speicherfrist eines Ereignisses (Straftat) ein neues Ereignis (Straftat) hinzukommt, beginnt die Prüffrist neu zu laufen Dies hat zur Folge, dass auch die vergangenen Ereignisse nunmehr der neuen Speicherungsfrist unterliegen.

Aus datenschutzrechtlicher Sicht ist diese Lösung unbefriedigend (siehe hierzu auch den 10. Tätigkeitsbericht des TLfDI unter Punkt 7.8).
Weitere Ausführungen finden sich im Leitfaden des TLfDI zu den Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut, der auf der Homepage des TLfDI (https://www.tlfdi.de/tlfdi/) unter dem Menüpunkt Themen / Orientierungshilfe abrufbar ist.

7.12 Mysteriöses Auftauchen personenbezogener Daten – War die Polizei involviert?

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie sich in ihrem Recht auf informationelle Selbstbestimmung verletzt sah.
Sie hegte den Verdacht, dass ein(e) Mitarbeiter(in) einer bestimmten Polizeidienststelle ihre derzeitige Wohnanschrift unerlaubt abgefragt und gegebenenfalls an eine dritte Person weitergegeben habe.
Daraufhin bat der TLfDI das Thüringer Landeskriminalamt um Mitteilung, ob jemand in der konkret benannten Polizeidienststelle in den durch die Meldebehörden zur Verfügung gestellten Daten eine Abfrage zu der Beschwerdeführerin getätigt habe. Das Thüringer Landeskriminalamt prüfte diese Protokolldatei auf Abfragen zu dem Namen der Beschwerdeführerin. Das Auswertungsergebnis ergab jedoch, dass kein Mitarbeiter der in Verdacht geratenen Polizeidienststelle eine solche Abfrage durchgeführt hatte. Eine nähere Zuordnung einer konkreten Abfrage zu der Beschwerdeführerin selbst war anhand der Protokolldatei nicht möglich. Da die Beschwerdeführerin gleichzeitig Strafanzeige erstattet hatte, liefen parallel auch die Ermittlungen der Staatsanwaltschaft. Ein Ermitt-

lungsverfahren wurde jedoch nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt, ein weiteres war bei Erstellung dieses Tätigkeitsberichtes noch nicht abgeschlossen.
Die Beschwerdeführerin wollte den Ausgang des zweiten Strafverfahrens abwarten und bat den TLfDI deshalb, in ihrem Fall vorerst nicht weiter tätig zu werden.

Fragt die Polizei Daten ab, muss für diese Abfrage eine Rechtsgrundlage oder ggf. eine Einwilligung der Betroffenen vorliegen. Sind diese Voraussetzungen nicht gegeben, ist das nicht nur datenschutzrechtlich zu beanstanden, sondern kann im schlimmsten Fall auch ein strafrechtliches Ermittlungsverfahren gegen den Abfragenden nach sich ziehen.

7.13 Abgefragt – Abfrage von Meldedaten durch die Polizei

Im Berichtszeitraum rief ein Beschwerdeführer den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an und berichtete, dass ein Angehöriger der Thüringer Polizei im Rahmen einer Zeugenvernehmung angegeben habe, die Wohnanschrift des Beschwerdeführers recherchiert zu haben.
Um den Sachverhalt aus datenschutzrechtlicher Sicht zu prüfen, bat der TLfDI die Landespolizeidirektion (LPD) zunächst um eine Stellungnahme. Aus dieser ging hervor, dass die besagte Abfrage im Rahmen eines Ermittlungsverfahrens der Staatsanwaltschaft Erfurt stattgefunden hatte. Der Polizeibeamte war grundsätzlich zur Abfrage der der Thüringer Polizei zur Verfügung gestellten Daten der Einwohner- und Meldeämter berechtigt. In dem Verfahren kam der Beschwerdeführer als Zeuge in Betracht. Die Polizei berief sich bei ihrem Handeln auf die Ermittlungsgeneralklausel des § 163 Strafprozessordnung (StPO) und wollte auf diesem Wege in Erfahrung bringen, wo der Betroffene wohnhaft war. Andere Ansatzmöglichkeiten besaß die Polizei aussagegemäß zum damaligen Zeitpunkt nicht. Aufgrund der Prüfung des Wohnortes hätte kein Zusammenhang mit dem Tatort vorgelegen, sodass die Daten des Beschwerdeführers keiner weiteren Verwendung bedurften. Die Polizei habe die Daten des Beschwerdeführers folglich weder in einer Akte noch in einer Datei gespeichert.
Um den Sachverhalt jedoch abschließend datenschutzrechtlich zu würdigen, nahm der TLfDI zusätzlich Akteneinsicht bei der Staats-

anwaltschaft Erfurt. Im Rahmen dieser Einsicht stellten sich für den TLfDI weitere Fragen. Zum einen war aus der staatsanwaltschaftlichen Ermittlungsakte noch nicht hinreichend erkennbar, dass das tatrelevante Dokument (ein anonymes Schreiben) an den Beschwerdeführer geschickt worden war. Zum anderen war dem TLfDI auch nicht hinreichend klar, aus welchem Grund die Polizei aufgrund der Wohnanschrift des Beschwerdeführers auf einen möglichen Täter hätte schließen können. Aus diesem Grund bat der TLfDI die LPD erneut um eine Stellungnahme und dabei insbesondere darum, konkret darzulegen, aus welchen Gründen die Datenabfrage zu dem Beschwerdeführer erforderlich war. Aus der erneuten Stellungnahme der LPD ergab sich zum einen, dass der Beschwerdeführer eine Kopie des anonymen Schreibens zumindest weitergeleitet hatte. Zum anderen erhielt der TLfDI Kenntnis darüber, dass der Beschwerdeführer im Bereich des möglichen Tatorts geboren wurde und deshalb ein Zusammenhang mit der Tat in Betracht kam. Nachdem die Polizei festgestellt hatte, dass der Beschwerdeführer dort nicht mehr wohnhaft war, verwarf sie weitere Ermittlungen. Die Daten des Beschwerdeführers bedurften somit keiner Verwendung und wurden weder in einer Akte abgelegt noch in einer Datei gespeichert.
Da für die Datenabfrage eine Rechtsgrundlage (§ 163 StPO) vorhanden war, lag ein Datenschutzverstoß im Ergebnis nicht vor.

Der TLfDI hat neben seinem Auskunftsanspruch gegenüber den öffentlichen Stellen gemäß § 38 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) auch die Möglichkeit, in deren Unterlagen und Akten sowie Datenverarbeitungsprogramme Einsicht zu nehmen. Nur so wird ihm eine umfangreiche Kontrollkompetenz ermöglicht. Damit der TLfDI nicht vor verschlossenen Türen steht, ist ihm darüber hinaus Zutritt zu allen Diensträumen zu gewähren.

7.14 Einnahme von Verwarngeldern als „olympische Disziplin“ der Polizei?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Information, dass bei der Einnahme von Bußgeldern durch die Thüringer Polizei jeweils der Name des zuständigen Polizeibeamten notiert würde. Dadurch wäre es möglich, nachzuvollziehen, in welcher Quantität der jeweilige Polizeibeamte Bußgelder eingenommen hat. Es stellte sich daher die

Frage, ob die von Polizeibeamten eingenommenen Verwarngelder als Leistungskriterium bzw. als Leistungskontrolle für diese verwendet würden.
Der TLfDI wandte sich an das damalige Thüringer Innenministerium und bat um eine Stellungnahme zu den Fragen, ob dieses Vorgehen für eine Leistungskontrolle genutzt werde, aus welchem Grund und auf welcher Rechtsgrundlage die Namen der Polizeibeamten notiert würden und wer Zugriff auf diese Daten habe.
Das TIM antwortete unter Beteiligung der Landespolizeidirektion (LPD) und teilte Folgendes mit:
Aufgrund eines Erlasses des TIM vom 21. Februar 2008 über die Beschaffung und Verwaltung der Verwarnungsgeldblöcke sowie die Abrechnung der Verwarngelder würden im Rahmen der Dienst- und Fachaufsicht regelmäßige Kontrollen dieser Blöcke sowie der Abrechnung der Verwarngelder von den Vorgesetzten durchgeführt und nachgewiesen. Die Dienststellenleiter bzw. Leiter der Organisationseinheiten seien dabei verpflichtet, in regelmäßigen Abständen die Geldannahmestelle/Zahlstelle (GASt/ZSt) und deren Nachweisunterlagen zu kontrollieren.
Zu diesen Nachweisunterlagen der GASt/ZSt gehöre auch die Verwaltung und Abrechnung der Verwarnungsgeldblöcke, worüber ein Bestandsnachweis geführt werde. Hierbei führe die GASt/Zst den Empfang, die Ausgabe, die Vereinnahmung und Weitergabe der Verwarnungsblöcke personenbezogen und listenmäßig auf.
Nach festgelegten Grundsätzen empfange der Bedienstete gegen Unterschrift auf dieser Bestandsübersicht einen Block, arbeite mit diesem und rechne jeweils vierzehntägig (in Ausnahmen auch monatlich oder nach Erreichen einer bestimmten eingenommen Geldsumme) mit der zuständigen Zahlstelle gegen Quittierung ab. Der Betrag werde in der Anschreibliste für Einnahmen der GASt/ZSt erfasst. Sobald der Block vollständig verbraucht oder eine Abgabe aus anderen Gründen (z. B. Versetzung) erforderlich sei, sei bei der GASt/ZSt abzurechnen, bei der er empfangen wurde.
Zugriff auf diese Daten hätten, so das TIM, die jeweiligen Verwalter der Geldannahmestelle und deren Stellvertreter sowie der Dienststellenleiter und dessen Stellvertreter sowie durch den Dienststellenleiter bzw. die LPD mit der Prüfung beauftragte Beamte.
Das TIM betonte, es bestehe keine Weisungslage, weder seitens des TIM noch der LPD, wonach die eingenommenen Verwarngelder als Leistungskriterium verwendet werden dürften.

Dies wäre nach Ansicht des TLfDI auch unzulässig. Der TLfDI verwies hierzu auf den damals geltenden § 89 Abs. 4 Thüringer Beamtengesetz (ThürBG), der für Polizisten als Beamte des Freistaates Thüringen gilt. Die Regelung des § 89 Abs. 4 ThürBG (alt) findet sich nach der Novellierung des ThürBG im August 2014 nunmehr in § 79 ThürBG wieder. Danach darf der Dienstherr nur dann personenbezogene Daten über Beamte erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.
An diesen Vorgaben gemessen, hielt der TLfDI eine Leistungskontrolle anhand der Quantität der eingenommenen Verwarngelder nicht für erforderlich und damit für unzulässig.
Eine Beanstandung gemäß § 39 Abs. 1 ThürDSG war vom TLfDI im Ergebnis jedoch nicht auszusprechen, da er keine Indizien dafür erkennen konnte, dass die Polizei eingenommene Verwarngelder tatsächlich als Leistungskriterium verwendete.
Sachdienliche Hinweise nimmt der TLfDI aber gern entgegen.

Die Namenskennung bei der Einnahme von Verwarngeldern seitens der Polizei ist datenschutzrechtlich dann unzulässig, soweit sie für die Leistungsüberprüfung von Polizeibeamten anhand eingenommener Verwarngelder vorgenommen wird. Dies ergibt sich aus § 79 Abs. 1 ThürBG. Sollte eine solche Überprüfung dennoch durchgeführt werden, haben Betroffene die Möglichkeit, sich an den TLfDI zu wenden.

7.15 DNA-Datei und Datenschutz

Das Thüringer Landeskriminalamt (TLKA) beabsichtigte im Berichtszeitraum die Einführung einer elektronischen Datenbank (DNA-Intern-Datei), in welcher DNA-Identifizierungsmuster von Mitarbeitern der Thüringer Polizei eingestellt werden sollen, die aufgabenbedingt häufig mit (Tatort-)Spuren zu tun haben. Diese Datei soll dem Abgleich mit der fallbezogenen Spurenmusterdatei und dem rechtzeitigen Erkennen von DNA-Spuren dienen, welche durch Personen, die mit der Suche, Sicherung und Analysierung dieser Spuren befasst sind, verursacht wurden (Trugspuren). Falsche

Ermittlungsansätze sollen dadurch ausgeschlossen werden. Der Abgleich solle nur fallbezogen mit den DNA-Identifizierungsmustern der für diesen Fall betrauten Mitarbeiter erfolgen. Bei einer Übereinstimmung solle dann die zuständige Kriminalpolizeiinspektion oder das TLKA benachrichtigt werden, um zu prüfen, ob der Mitarbeiter tatsächlich den Fall bearbeitet hatte. Stimmt der Sachverhalt überein, soll die DNA-Spur des betroffenen Mitarbeiters in der fallbezogenen Spurenmusterdatei gelöscht werden.

Die Aufnahme der DNA-Identifizierungsmuster der Personen in die DNA-Intern-Datei solle dabei ausschließlich auf freiwilliger Basis erfolgen und jederzeit widerrufbar sein. Im Rahmen seiner Beratungsfunktion gemäß § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) wurde auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bei der Einführung der DNA-Intern-Datei beteiligt. Von erheblicher Bedeutung war für den TLfDI die Freiwilligkeit der DNA-Abgabe, da in Thüringen mangels gesetzlicher Grundlage für einen DNA-Abgleich die Entscheidung darüber nur beim Betroffenen selbst liegen kann. Der Dienstherr bzw. der Arbeitgeber kann keinen Mitarbeiter verpflichten, eine solche Probe abzugeben. Es muss daher eine freiwillige, schriftliche und informierte Einwilligung des Betroffenen vorliegen. Da eine freiwillige Einwilligung eines Arbeitnehmers aus Sicht des TLfDI vor dem Hintergrund eines bestehenden Abhängigkeitsverhältnisses kritisch gesehen wird, dürfen die Verweigerung sowie der Widerruf der Einwilligung keine negativen beruflichen Folgen nach sich ziehen. So darf zum Beispiel ein Beschäftigter, der nicht einwilligen möchte, nicht aus diesem Grund aus seinem Arbeitsfeld in ein anderes umgesetzt oder versetzt werden. Eine Beteiligung des Hauptpersonalrates sah der TLfDI angesichts der sensiblen Thematik als unabdingbar an.

Die Änderungsvorschläge des TLfDI zu einem vorgelegten Entwurf einer Einwilligungserklärung wurden vom TLKA berücksichtigt, so zum Beispiel, dass in den einmaligen Abgleich mit der DNA-Analyse-Datei beim BKA gesondert eingewilligt werden muss. Weiterhin wies der TLfDI darauf hin, dass der Kreis der Betroffenen im Verfahrensverzeichnis genau zu konkretisieren sei. Dies wurde vom TLKA umgesetzt. Die Höchstspeicherungsfrist wurde zudem von zwei Jahren auf ein Jahr heruntergesetzt. Mit den vom TLKA vorgenommen Änderungen ist die Führung der DNA-Intern-Datei datenschutzrechtlich vertretbar. Jedoch behält sich der TLfDI eine Nach-

kontrolle zur Prüfung der Einhaltung der datenschutzrechtlichen Anforderungen hinsichtlich der DNA-Intern-Datei und ihrer Umsetzung vor. Dabei wird auch die Weiterentwicklung der DNA-Analysemethoden zu beachten sein.

Eine Datenverarbeitung ist gemäß § 4 Abs. 1 Satz 1 ThürDSG immer dann zulässig, wenn eine Rechtsvorschrift diese erlaubt oder der Betroffene in die Datenverarbeitung und/oder -nutzung eingewilligt hat. Fehlt wie im Fall der DNA-Intern-Datei eine gesetzliche Ermächtigungsgrundlage, kommt nur eine Einwilligung in Betracht. Dabei ist zwingend zu beachten, dass diese auf freiwilliger Basis erfolgt.

7.16 Zentrum für Überwachung

Auf dem Gebiet der polizeilichen Überwachung der Telekommunikation wollen die Länder Berlin, Brandenburg, Sachsen-Anhalt, der Freistaat Sachsen und der Freistaat Thüringen ein Gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ) errichten. Dessen Wirkbetrieb soll ab dem Jahr 2018 aufgenommen werden. Das GKDZ soll als Anstalt des öffentlichen Rechts auf der Grundlage eines Staatsvertrags errichtet werden. Da in dem GKDZ höchstwahrscheinlich viele sensible personenbezogene Daten aus fünf Bundesländern verarbeitet werden sollen, sind hohe Anforderungen an den Datenschutz und die Datensicherheit zu stellen.
Da aber neben einem Staatsvertragsentwurf weitere konkrete Konzepte für die tatsächliche Ausgestaltung des GDKZ dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bisher nicht vorliegen bzw. überhaupt noch nicht erstellt wurden, kann der TLfDI eine weitergehende datenschutzrechtliche Beurteilung des GDKZ derzeit noch nicht vornehmen.
Zu dem Entwurf des Staatsvertrages zwischen den teilnehmenden Ländern nahm der TLfDI Stellung und wies unter anderem darauf hin, dass der Aufgabenumfang des GKDZ im Staatsvertrag konkret festzulegen sei, dass die jeweiligen Polizeibehörden in dem GKDZ nur auf ihre eigene Datensätze Zugriff haben dürften und dass die bei einer Telekommunikationsüberwachung erhobenen Daten nach dem jeweiligen Stand der Technik entsprechend zu verarbeiten seien. Der TLfDI wies – gerade im Lichte des ergangenen Urteils des EuGH vom 6. Oktober 2015 C-262/14 (Safe Harbor) – nochmals darauf hin,

dass beispielsweise bei der Vergabe etwaiger Unteraufträge durch das GKDZ (z. B. bei Wartungsaufträgen) eine Datenübermittlung in die USA grundsätzlich bedenklich sei. Auch muss die eingesetzte Hard- und Software europäischen Standards entsprechen.
Der TLfDI wird das Projekt datenschutzrechtlich intensiv betreuen.

Das Gemeinsame Kompetenz- und Dienstleistungszentrum soll auf der Grundlage eines Staatsvertrages zwischen den Ländern Berlin, Brandenburg, Sachsen-Anhalt, dem Freistaat Sachsen und dem Freistaat Thüringen als Anstalt des öffentlichen Rechts errichtet werden. Im Rahmen der Datenverarbeitung in diesem Zentrum ist insbesondere darauf zu achten, dass die jeweiligen Polizeibehörden nur auf ihre eigene Datensätze Zugriff haben dürfen und dass die bei einer Telekommunikationsüberwachung erhobenen Daten nach dem jeweiligen Stand der Technik zu verarbeiten sind. Die frühzeitige Beteiligung des Datenschutzbeauftragten ist angeraten.

7.17 „Body-Cams“ für den modernen Polizisten – chic, aber auch zulässig?

Im Berichtszeitraum testeten mehrere Bundesländer in Pilotprojekten den Einsatz von „Body-Cams“ bei der Polizei. Eine „Body-Cam“ ist eine kleine Videokamera, die der Polizei dazu dienen soll, im Rahmen ihrer Einsätze das Einsatzgeschehen direkt aufzeichnen und somit später auswerten zu können.
Zum möglichen Einsatz von „Body-Cams“ in Thüringen stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beim damaligen Thüringer Innenministerium (TIM) die Anfrage, ob ein solches Pilotprojekt auch in Thüringen Anwendung finde. In seiner kurzen Antwort teilte das TIM dem TLfDI mit, dass derzeit weder „Body-Cams“ im Einsatz noch zukünftig geplant seien.
Parallel dazu diskutierten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von „Body-Cams“. Im Ergebnis sind die Datenschützer grundsätzlich der Auffassung, dass für den Einsatz von „Body-Cams“ eine Rechtsgrundlage erforderlich sei. In dieser sollten die Voraussetzungen für den Einsatz und auch für die weitere Verarbeitung (z. B. die Auswertung und Löschung der Daten) geregelt werden.

Der TLfDI hat Verständnis für die Argumente aus den Reihen der Polizeigewerkschaften, dass „Body-Cams“ auch bei Thüringer Polizei zum Einsatz kommen sollen. Ein Einsatz solcher „Body-Cams“ zum Schutz der Polizeibeamten bei Personen- oder Fahrzeugkontrollen an öffentlich zugänglichen Orten ist bereits jetzt nach § 33 Abs. 6 Satz 1 Polizeiaufgabengesetz (PAG) möglich.
Sofern der Einsatz der „Body-Cams“ über den Eigensicherungszweck der Polizisten hinausginge, wäre der Zweck der Aufzeichnung hinreichend klar im PAG zu regeln. Dabei wären in jedem Fall auch beschäftigtendatenschutzrechtliche Fragen zu erörtern und zu klären.

7.18 Polizist verkauft Privat-PC mit Dienst-Daten

Wer heutzutage einen gebrauchten Personal Computer (PC) in einem Elektrofachgeschäft kauft, sollte nicht nur mit äußerlichen „Gebrauchsspuren“ des PCs rechnen. Er kann leider auch nicht selten auch noch einige personenbezogene Daten vom Vorbesitzer des PCs finden. So erging es auch einem Inhaber eines Mediaunternehmens. Dieser hatte sich bei einem Elektrofachgeschäft einen gebrauchten PC gekauft. Erstaunlich war nicht nur der günstige Preis. Auch die Daten, die auf dem PC zu finden waren, überraschten ihn so sehr, dass er seinen „Fund“ dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) meldete. Auf dem PC befanden sich tatsächlich über 1.000 Dateien, die einen polizeirelevanten Hintergrund hatten.
Daraufhin hakte der TLfDI bei der Landespolizeidirektion (LPD) nach, welche Regelungen dort für den Umgang mit dienstlichen Dateien auf privaten PCs gälten. Die LPD teilte daraufhin mit, dass es sich bei dem Vorbesitzer des PCs um einen Polizeibeamten einer Polizeiinspektion handelte, der sich jedoch schon seit einigen Jahren im Ruhestand befände. Es gäbe bei der Polizei keine dienstliche Regelung, die erlaube, dass das Speichern von dienstlichen Dateien auf privaten PCs zulässig sei; auch die Möglichkeit der Telearbeit bestünde nicht. Vielmehr verwies die LPD auf die Dienstanweisung Nr. 1/2008 für den Umgang mit IT-Systemen, nach der es jedem Anwender und Polizisten untersagt ist, dienstliche Software bzw. dienstliche Dateien auf privater Hardware zu nutzen. Bei der Versetzung eines Polizeibeamten in den Ruhestand erfolge ferner eine Belehrung, unter anderem zur Treue- und Verschwiegenheitspflicht, zur Herausgabe amtlicher Unterlagen sowie zu den Folgen der

Nichterfüllung (z. B. disziplinarrechtliche Ahndung, vermögensrechtliche Haftung).
Das dafür verwendete Formblatt „Erklärung bei Versetzung in den Ruhestand“ hielt einer datenschutzrechtlichen Prüfung durch den TLfDI nicht stand: Er monierte die veralteten Rechtsnormen, auf die in dem Formblatt verwiesen wurde und regte an, dass Beamte bei Ausscheiden aus dem Polizeidienst künftig auch erklären müssten, nicht im Besitz von Dateien über dienstliche Vorgänge zu sein.
Der TLfDI informierte daraufhin das damalige Thüringer Innenministerium (TIM) als übergeordnete Stelle über diesen Vorfall. Er bat darum, dass nochmals alle Polizeibeamten über den Umgang von dienstlichen Daten belehrt würden und regte die Prüfung der Einleitung disziplinarischer Maßnahmen an.

Die Polizei hat zu gewährleisten, dass Polizisten bei Ausscheiden aus dem aktiven Dienst keine dienstlichen Akten oder Dateien auf privaten Datenträgern „mit nach Hause nehmen“. Sofern ein Polizist gegen diese Pflicht verstößt, riskiert er mindestens, dafür disziplinarrechtlich belangt zu werden. Ein anderes Problem betrifft die Frage, wie PCs, Laptops und Smartphones im Falle eines Weiterverkaufs wirklich „clean“ gemacht werden können, also frei von personenbezogenen Daten des Verkäufers sind. Der TLfDI hat zu der Problematik in einer Pressemitteilung „Sind sie noch da?“ auf das sichere Löschen von Daten hingewiesen. Die Pressemitteilung des TLfDI vom 06.06.2016 findet sich in der Anlage 52 zu diesem Tätigkeitsbericht.

7.19 Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit

Die Thüringer Polizei beabsichtigt, ein speziell auf die kriminalpolizeiliche Arbeit bezogenes automatisiertes Verfahren namens Fallbearbeitungssystem (FBS-TH) einzuführen, welches neben dem bereits bestehenden Vorgangsbearbeitungssystem (VBS) existieren und kriminalpolizeiliche Zusammenhänge von unterschiedlichen Fällen aufzeigen soll. Dazu sollen Datensätze zu Verfahren aus dem VBS als Fälle zum Hauptverfahren im FBS-TH übernommen werden, sofern der Sachbearbeiter einen möglichen Zusammenhang zum Hauptverfahren erkannt hat. Diese Daten sollen im FBS-TH elektro-

nisch recherchierbar vorgehalten werden, bis das Hauptverfahren abgeschlossen ist.
Der TLfDI wies zu dem geplanten Fallbearbeitungssystem FBS-TH im Berichtszeitraum unter anderem auf Folgendes hin: Es sei zunächst konkret festzulegen, welche Mitarbeiter die Verfahren im FBS-TH bearbeiten dürfen. Damit das FBS-TH ein Fallbearbeitungssystem bleibt, das kriminalpolizeiliche Zusammenhänge von unterschiedlichen Fällen aufzeigen und laut der Aussage der Polizei nur neben dem bestehenden Vorgangssystem Anwendung finden soll, empfahl der TLfDI, das System nur bei Straftaten bzw. Gefahren im Bereich der schweren Kriminalität bzw. von erheblicher Bedeutung (Anhaltspunkte könnten hier beispielsweise die Katalogstraftaten der §§ 98a, 100a, StPO geben) einzusetzen. Es bedürfe in jedem Fall einer sorgfältigen Prüfung des Einzelfalles. Bei jeder Übernahme eines Falles müsse die Erforderlichkeit der Übernahme in das FBS-TH begründet und die entsprechende Rechtsgrundlage angegeben werden. Dies sei zu dokumentieren. Der Dienststellenleiter müsse seine Zustimmung erteilen und ggf. den zuständigen behördlichen Datenschutzbeauftragten (bDSB) beteiligen. Es müsse ferner sichergestellt werden, dass das FBS-TH nicht für Bagatelldelikte und somit schlussendlich für fast jedes Delikt bzw. jede Gefahrenlage genutzt werde. Die in das FBS-TH übernommenen Daten seien vor einer Übernahme zu kennzeichnen. Nach der Übernahme müsse zudem ausgeschlossen werden, dass inhaltliche Änderungen oder Ergänzungen der übernommenen Daten vorgenommen werden könnten. Für diese Daten dürften demnach nur noch Leserechte bestehen. Hierfür seien die erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Die Kennzeichnung der übernommenen Daten umfasse auch die jeweilige Angabe der Rechtsgrundlage dieser Datenverarbeitung. Zu beachten sei des Weiteren, dass die Weiterverwendung der durch bestimmte Ermittlungsmaßnahmen gewonnenen Daten zu anderen Zwecken als jenen, für die sie im Ausgangsverfahren erhoben wurden, nur im Rahmen der gesetzlichen Vorschriften gestattet sein dürfe. Generell sei zu gewährleisten, dass die prozessualen Anforderungen an die Verarbeitung und Nutzung der erhobenen Daten erfüllt würden.
Vorgänge, die seit einem Jahr nicht mehr bearbeitet werden, sind aus Sicht des TLfDI (bestenfalls automatisch) auf inaktiv zu setzen. Ist ein Vorgang auf inaktiv gesetzt worden, sollte eine weitere Bearbei-

tung nicht mehr möglich sein und die verantwortliche Stelle hat die Erforderlichkeit einer weiteren Speicherung zu überprüfen.
Schließlich ist auch die gesetzliche Auskunftspflicht gemäß § 47 Polizeiaufgabengesetz (PAG) zu beachten, wonach der Betroffene auch Auskunft zu den in diesem System gespeicherten Daten zu seiner Person erhält.
Der TLfDI wird im Rahmen einer Nachkontrolle das Fallbearbeitungssystem auf seine Vereinbarkeit mit dem Datenschutzrecht überprüfen. Darüber wird der TLfDI im kommenden Tätigkeitsbericht informieren.

Die Polizei hat – aufgabenbedingt – Zugang zu einer Fülle von personenbezogenen Daten. Jedoch darf auch sie nicht sämtliche Daten sammeln und auswerten. Gerade bei einem Fallbearbeitungssystem wie FBS-TH hat die verantwortliche Stelle sorgfältig zu prüfen, welche Fälle in das Fallbearbeitungssystem aufgenommen werden. Dies ergibt sich nicht zuletzt aus dem Gebot der Datensparsamkeit gemäß § 1 Abs. 2 Satz 1 Thüringer Datenschutzgesetz.

7.20 Beglaubigte Personalausweiskopien – zukünftig nicht mehr nötig

Nach § 47 Abs. 1 Satz 1 Polizeiaufgabengesetz (PAG) erteilt die Polizei dem Betroffenen auf Antrag grundsätzlich über die zu seiner Person gespeicherten Daten Auskunft.
Im Rahmen der Antragsstellung verlangte die Thüringer Polizei bisher immer eine beglaubigte Personalausweiskopie des Betroffenen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sah im Gegensatz dazu die Anforderung einer einfachen Ausweiskopie als ausreichend an. Unberührt hiervon bleibt die persönliche Identifizierung des Antragstellers auf der Polizeidienststelle. Die Anforderung einer beglaubigten Ausweiskopie ist für die Erreichung des Zwecks der Vermeidung einer Auskunftserteilung an einen unberechtigten Dritten ungeeignet. Eine beglaubigte Kopie bzgl. des Identitätsnachweises besitzt gegenüber einer einfachen Kopie keinen Mehrwert, da sie letztlich nur bestätigt, dass die Kopie mit dem Original übereinstimmt. Eine beglaubigte Personalausweiskopie an sich stellt somit nicht sicher, dass tatsächlich keine unberechtigte Person Kenntnis vom Inhalt des Aus-

kunftsersuchens erlangt. Diese Gefahr einer falschen Versendung könnte unter Umständen lediglich mithilfe eines Einschreibens (mit Rückschein) minimiert werden.
Dem Auskunftsersuchen des Bürgers mit der Forderung nach einer beglaubigten Ausweiskopie werden nach Ansicht des TLfDI zu hohe Hürden auferlegt, die den Antrag, eine Auskunftserteilung von der Polizei als öffentliche Stelle zu erhalten, deutlich erschweren.
Vom TLfDI dazu um Stellungnahme gebeten, teilte das Thüringer Ministerium für Inneres und Kommunales (TMIK) mit, dass es erwäge, dieser Auffassung des TLfDI zu folgen, sodass eine beglaubigte Ausweiskopie für die Antragstellung grundsätzlich nicht mehr erforderlich wäre. Eine solche beglaubigte Kopie könnte dann nur noch in Ausnahmefällen von der Polizei gefordert werden, z. B. wenn ein Manipulationsverdacht an der Kopie bestünde.

Bei einem schriftlichen Auskunftsersuchen gemäß § 47 PAG sollte der Betroffene nach Auffassung des TLfDI zukünftig grundsätzlich keine beglaubigte Personalausweiskopie mehr vorlegen müssen. Eine einfache Kopie reicht dafür grundsätzlich aus. Einzelne Datenfelder auf der Personalausweiskopie kann der Betroffene zudem schwärzen, da sie für die Identifizierung nicht erforderlich sind (z. B. Ausweisnummer, Größe, Augenfarbe). Spricht der Antragsteller persönlich bei der Polizeidienststelle vor, wird regelmäßig keine Ausweiskopie erforderlich sein. Ein Vermerk, dass die Identität des Antragstellers geprüft wurde, reicht aus.

7.21 Polizeiliche Erfassung von Ausweisdaten per Smartphone-Foto?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage eines Bürgers, der beobachtet hätte, dass eine ausländische Familie von zwei uniformierten Bediensteten der Bundespolizei kontrolliert worden sei. Im Rahmen der Identitätsfeststellung sei mindestens ein Ausweisdokument der Familie von den Polizeibeamten mithilfe eines Smartphones bildlich erfasst worden. Der Bürger bat um Prüfung, ob dieses Vorgehen der Polizei datenschutzrechtlich zulässig gewesen sei.
Da es sich bei den Polizeibeamten um Bedienstete der Bundespolizei gehandelt haben soll und für diese Bundesbehörde die Bundesbeauf-

tragte für den Datenschutz und die Informationsfreiheit (BfDI) sachlich zuständig ist, gab der TLfDI die weitere datenschutzrechtliche Prüfung an die BfDI ab.
Gleichzeitig nahm der TLfDI diese Bürgeranfrage aber zum Anlass, zu ermitteln, ob die Thüringer Polizei Smartphones zur bildlichen Erfassung von Ausweisdokumenten heranzieht.
Die Rückmeldung der Thüringer Landespolizeidirektion ergab zunächst, dass die Nutzung privater Mobiltelefone bei ihren Bediensteten im Dienst untersagt sei.
Im Hinblick auf die dienstlich bereitgestellten Mobiltelefone sei eine Sperrung von Einzelfunktionen –wie beispielsweise die Kamerafunktion – nicht möglich. Deswegen sei die Möglichkeit, mit dienstlich zur Verfügung gestellten Geräten Ausweisdokumente bildlich zu erfassen, theoretisch nicht ausgeschlossen.
Aus Sicht der Landespolizeidirektion sei das Fotografieren von Ausweisdaten zur polizeilichen Aufgabenerfüllung jedoch weder erforderlich noch verhältnismäßig.
Die der Landespolizeidirektion nachgeordneten Behörden seien angewiesen, deren Bedienstete in dieser Frage hinreichend zu sensibilisieren und die Benutzung von Mobiltelefonen für das Fotografieren von Ausweisdaten zu untersagen.
Im Rahmen der Identitätsfeststellung sei es im Aufgabenkreis der Thüringer Polizei unzulässig, dass Polizeibeamte Ausweisdokumente von Bürgern bildlich erfassen.
Es genügt, wenn der Betroffene dem Polizeibeamten zur Feststellung der Identität seine Ausweispapiere zur Prüfung aushändigt (§ 14 Abs. 2 Satz 2 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei). Das Erheben und das Verwenden personenbezogener Daten aus einem Personalausweis ist mit dem aktuellen Personalausweisgesetz (PAuswG) abschließend gesetzlich geregelt (§§ 14 ff. PAuswG). Bei einer Identifizierung anwesender Personen aus polizeierkennungsdienstlichen Gründen ist eine Kopie nicht erforderlich und damit unzulässig. Einige Gesetze und Verordnungen hingegen sehen eine ausdrückliche Ermächtigung zum Kopieren des Ausweises vor. Für Banken gilt beispielsweise § 8 Abs. 1 Satz 3 Geldwäschegesetz, und für Telekommunikationsanbieter (z. B. beim Handyvertrag) § 95 Abs. 4 Satz 2 TKG.

Eine Ablichtung oder eine Speicherung des Ausweises – auch mittels der Verwendung von Funktionen „Speicherung und Bildwiedergabe

eines Smartphones – durch die Polizei wird weder von der gesetzlichen Regelung des PAuswG noch von einer anderen im vorliegenden Fall anwendbaren Vorschrift erfasst und verstößt daher gegen § 4 Abs. 1 Thüringer Datenschutzgesetz.

Das Erheben und das Verwenden personenbezogener Daten aus einem Personalausweis ist mit dem aktuellen PAuswG abschließend gesetzlich geregelt (§§ 14 ff. PAuswG). Die Anfertigung von Kopien des Personalausweises anlässlich einer Polizeikontrolle – vorliegend mittels Erfassung von Ausweisdaten per Smartphone-Foto – ist vom Gesetzgeber nicht vorgesehen; somit ist sie auch nicht zulässig.

7.22 Kennzeichenerfassung auf Hotelparkplatz

Ein Hotelbetreiber wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass auf seinem Hotelparkplatz in regelmäßigen Abständen von der Polizei die Kennzeichen der parkenden Autos aufgenommen würden. Da ihm mündlich keine Auskunft zum Zweck der Datenerhebung gegeben worden sei, bat er beim TLfDI um Klärung dieses für ihn seltsam anmutenden Sachverhalts.
Der TLfDI fragte dazu bei der zuständigen Landespolizeiinspektion (LPI) an, auf welcher Rechtsgrundlage und zu welchem Zweck die Datenerhebung stattgefunden habe. Ausführlich nahm die Landespolizeiinspektion Stellung in dieser Angelegenheit und teilte dem TLfDI mit, das besagte Hotel sei bei der Polizei dafür bekannt, dass dort seit Jahren rechtsextremistische Veranstaltungen stattfänden und es wiederholt zur Verübung von Straftaten gekommen sei. Die Datenerhebung in Form der Erfassung von Kfz-Kennzeichen stützte die LPI auf § 33 Abs. 1 und 3 Polizeiaufgabengesetz (PAG): Danach kann die Polizei personenbezogene Daten auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder Aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Gem. § 33 Abs. 3 Satz 1 PAG darf die Datenerhebung auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

Nachfragenswert war für den TLfDI jedoch, ob und wie die LPI im Rahmen ihrer Verhältnismäßigkeitsprüfung zur polizeilichen Datenerhebung berücksichtigte, dass nicht sämtliche auf dem Parkplatz befindlichen Fahrzeuge rein vorsorglich überprüft werden mussten, da der Parkplatz auch von anderen Hotelgästen genutzt wird/wurde, von denen eine Gefahr für die öffentliche Sicherheit und Ordnung grundsätzlich nicht angenommen werden kann bzw. konnte.
Die LPI wies nachfolgend darauf hin, dass sie im Rahmen der Prüfung der Angemessenheit die Interessen der polizeilichen Aufgabenerfüllung (Präventivwirkung im Hinblick auf politisch motivierte Straftaten) und das Recht auf informationelle Selbstbestimmung Unbeteiligter (Kennzeichen- bzw. Halterprüfung auf rechtsextremistischen Bezug) abgewogen habe. Dabei sei die LPI zu dem Ergebnis gelangt, dass im Zusammenhang mit der Datenerhebung von Kfz-Kennzeichen der Eingriff in das Recht auf informationelle Selbstbestimmung Unbeteiligter geringer zu bewerten sei, gerade weil ein milderes Mittel als die Datenerhebung in Form der Kennzeichenerfassung vorliegend nicht erkennbar war.
Gegen diese rechtliche Begründung hatte der TLfDI keine Einwände.

An dieser Stelle zeigt sich wieder einmal, dass Datenschutz keineswegs Täterschutz oder – hier genauer – Störerschutz ist. Dem TLfDI obliegt die Aufgabe, genau darauf zu achten, ob es für eine Datenerhebung einer öffentlichen Stelle eine Rechtsgrundlage im Sinne von § 4 Abs. 1 Satz 1 ThürDSG gibt und ob diese Datenerhebung erforderlich und angemessen im Sinne des Verhältnismäßigkeitsprinzips als Ausdruck rechtsstaatlichen Handelns gewesen ist. Liegen diese Voraussetzungen vor, so hat auch der TLfDI „nichts zu meckern“ – jedenfalls meistens.

7.23 Polizei vs. Polizei – Verfahren bei Dienstaufsichtsbeschwerden

Ein Polizeibeamter erfuhr in einem Personalgespräch, dass gegen ihn wegen seines dienstlichen Verhaltens eine Beschwerde vorliege. Er wurde zunächst einer anderen Aufgabe bzw. Dienstverrichtung zugewiesen. Der Polizist beauftragte einen Rechtsanwalt mit der Wahrnehmung seiner Interessen, der in Wahrnehmung seines Mandats Akteneinsicht beantragte, um auf das Vorgehen der Dienststelle

und die Vorwürfe entsprechend reagieren zu können. Von der zuständigen Landespolizeiinspektion (LPI) erhielt der Anwalt die Antwort, bei den eingeleiteten Verwaltungsermittlungen gegen seinen Mandanten handele es sich um formlose innerdienstliche Ermittlungen zur Klärung eines Beschwerdegegenstandes. Um den Ermittlungszweck nicht zu gefährden, könne eine Akteneinsicht zum derzeitigen Zeitpunkt nicht gewährt werden. Wegen Auskunftsverweigerung wandte sich der Polizist an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), der die LPI zur datenschutzrechtlichen Prüfung um Stellungnahme anschrieb.

Die LPI teilte mit, dem Betroffenen seien in einem Personalgespräch die erhobenen Vorwürfe ohne Angaben zu den Beschwerdeführern eröffnet und ihm Gelegenheit gegeben worden, sich dazu zu äußern. Da die Vorwürfe etwas unkonkret gewesen seien, seien zusätzliche Verwaltungsermittlungen auf der Grundlage der Dienstanweisung zur Behandlung von Aufsichtsbeschwerden gegen Angehörige der Thüringer Polizei im Geschäftsbereich der Landespolizeidirektion (DA-DAB) und der Dienstanweisung zur Behandlung von Disziplinarangelegenheiten im Geschäftsbereich der Landespolizeidirektion (DA-Diszi) unerlässlich gewesen. Die Akteneinsichtsverweigerung und damit die Auskunftsverweigerung stützt man auch auf die Grundlage des § 13 Abs. 5 Nr. 1 und 5 des Thüringer Datenschutzgesetzes, wonach eine Auskunft unterbleibt, soweit die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben gefährden würde und schützenswerte Interessen Dritter betroffen sind. Man wollte nämlich ein unbefangenes Aussageverhalten im Erkenntnisprozess sicherstellen und eine Einflussnahme Dritter unter dem Hinweis auf die noch laufenden Verwaltungsermittlungen ausschließen. Die Verwaltungsermittlungen habe man zwischenzeitlich abgeschlossen und alle gefertigten Unterlagen zuständigkeitshalber dem Präsidenten der LPD übersandt.

Um das Vorliegen der Voraussetzungen für eine Akteneinsichts- oder Auskunftsverweigerung zu überprüfen, nahm der TLfDI in Wahrnehmung seiner gesetzlichen Befugnisse Einsicht in den Beschwerdevorgang. Aus der Akte war zu entnehmen, dass man besagte Verwaltungsermittlungen angestellt hatte. Zu diesem Zweck wurde ein Ermittlungsführer bestellt, der die bei dem Ereignis, bei dem der Betroffene sich nicht angemessen verhalten haben sollte, anwe-

senden Personen als Zeugen befragte. Dabei war deutlich gemacht worden, dass es sich um keine polizeiliche Befragung, also nicht um ein strafrechtlich relevantes Ermittlungsverfahren mit Zeugenvernehmung gehandelt habe. Dass bei dieser Zeugenbefragung nicht erforderliche Informationen erhoben worden waren, konnte vom TLfDI nicht festgestellt werden. Zum Zeitpunkt der Akteneinsicht war die Prüfung durch die LPD, ob ein Disziplinarverfahren gegen den Polizisten eingeleitet werden sollte, bereits abgeschlossen. Der Abschlussvermerk, nach dem ein Disziplinarverfahren nicht eröffnet werden sollte, war jedoch noch nicht von der zur Mitzeichnung vorgesehenen LPI unterzeichnet. Dem Rechtsanwalt wollte man Akteneinsicht nach der Schlusszeichnung des Abschlussvermerks gewähren.

Das Vorgehen der Polizei, dass nur eine Verwaltungsermittlung, aber nicht gleich ein Disziplinarverfahren eingeleitet worden war, wurde damit begründet, dass ein Disziplinarverfahren für den Betroffenen weit schwerwiegender sei. Bei der Vielzahl von Beschuldigungen und Strafanzeigen sowie Dienstaufsichtsbeschwerden gegen Polizeibeamte soll daher immer erst festgestellt werden, ob der Sachverhalt konkrete Anhaltspunkte für die Einleitung eines förmlichen Disziplinarverfahrens biete. Dieses Vorverfahren sei auch in der Kommentierung zu § 17 Bundesdisziplinargesetz als von der Rechtsprechung zugelassen aufgeführt. Hiervon mache man zum Schutz der Bediensteten Gebrauch.

Im Ergebnis der datenschutzrechtlichen Prüfung hat der TLfDI ausgeführt, es bestehe, da es sich weder formell noch gewollt um ein förmliches Disziplinarverfahren gehandelt hatte, grundsätzlich ein Anspruch auf Akteneinsicht nach § 29 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG). Nach § 29 Abs. 1 ThürVwVfG hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Nach § 29 Abs. 2 ThürVwVfG ist die Behörde hierzu jedoch nicht verpflichtet, soweit durch die Akteneinsicht die ordnungsgemäße Erfüllung der Aufgabe beeinträchtigt wird. Der gegenüber dem Rechtsanwalt angeführte Grund, den Ermittlungszweck nicht zu gefährden, findet sich zwar in polizeilichen Vorschriften, nicht jedoch in § 29 ThürVwVfG. Polizeiliche Vorschriften kommen in diesem Zusammenhang aber nicht zur Anwendung, da keine polizeiliche Aufgabe nach dem Thüringer Polizeiaufgabengesetz vorlag und auch nicht die

Aufklärung und Verfolgung einer Straftat in Rede stand. Die letztendliche Entscheidung über die Einleitung eines Disziplinarverfahrens durch die LPD stand noch aus. Der Betroffene oder dessen Rechtsanwalt hatte nach § 29 Abs. 1 Satz 2 VwVfG lediglich kein Einsichtsrecht in Entwürfe von Entscheidungen. Eine nähere Begründung, weshalb die Einsicht in den gesamten Verwaltungsvorgang vor Unterzeichnung des Abschlussvermerks durch den Rechtsanwalt des Betroffenen den Untersuchungszweck gefährdet hätte, war aus dem Vorgang nicht zu entnehmen. Sobald jedoch der Abschlussvermerk unterzeichnet war, war auch hierzu die Auskunft bzw. Akteneinsicht zu gewähren. Dem kam die LPD zwischenzeitlich nach und teilte dem TLfDI nach einer weiteren Prüfung mit, dass rückblickend auch aus ihrer Sicht keine durchgreifenden Gründe vorlagen, die die Ablehnung der Akteneinsicht durch den Rechtsanwalt hätten rechtfertigen können. Es hätte also dem Antrag des Rechtsanwalts auf Akteneinsicht zunächst von der LPI und anschließend auch von der LPD nachgekommen werden müssen. Die LPD sagte zu, den Fall zum Anlass zu nehmen, den Geschäftsbereich diesbezüglich zu sensibilisieren.

In einem Verwaltungsverfahren hat der Betroffene bzw. dessen Anwalt das Recht auf Akteneinsicht nach § 29 ThürVwVfG. Hiervon ausgenommen sein können Entwürfe von Entscheidungen. Das Verwaltungsverfahren kennt keine polizeilichen Vorschriften nachgebildete Gründe, die Akteneinsicht zu verweigern. Führen Polizeidienststellen Verwaltungsverfahren, dürfen sie nicht ergänzend auf polizeiliche Vorschriften zurückgreifen.

Grunge Stempel rot VERTRAULICH – © Daniel Ernst / Fotolia.com

8 Verfassungsschutz

8.1 Bekanntgabe personenbezogener Daten durch das Amt für Verfassungsschutz – nicht ohne den TLfDI

Am 1. Januar 2015 trat das neue Thüringer Verfassungsschutzgesetz (ThürVerfSchG) in Kraft. Das Gesetz beinhaltet eine bundesweit einmalige Regelung zur Öffentlichkeitsarbeit des Amtes für Verfassungsschutz (AfV) unter Beteiligung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Nach § 5 Abs. 2 ThürVerfSchG hat das Amt für Verfassungsschutz auch die Aufgabe, die Öffentlichkeit in zusammenfassenden Berichten sowie in Einzelanalysen über Bestrebungen und Tätigkeiten, die sich gegen die freiheitliche demokratische Grundordnung richten, zu unterrichten. Es tritt solchen Bestrebungen und Tätigkeiten auch durch Angebote zur Information entgegen. Dabei dürfen der Öffentlichkeit personenbezogene Daten bekannt gegeben werden, wenn das Interesse an der Unterrichtung das schutzwürdige Interesse des Betroffenen überwiegt. Vor einer erstmaligen Bekanntgabe personenbezogener Daten ist dem TLfDI Gelegenheit zur Stellungnahme zu geben. Praktische Bedeutung erlangte die Beteiligung des TLfDI, als

kurze Zeit nach dem Inkrafttreten des ThürVerfSchG der Verfassungsschutzbericht zur Veröffentlichung vorbereitet werden sollte. In diesem würden erstmalig personenbezogene Daten bekannt gegeben werden. Das AfV legte dem TLfDI ausreichend dar, dass das Interesse an der Unterrichtung das schutzwürdige Interesse der Betroffenen überwog. Somit war es für den TLfDI nachvollziehbar, dass die personenbezogenen Daten im Rahmen der durch das AfV vorgenommenen Abwägung im Verfassungsschutzbericht genannt wurden.

Seit dem 1. Januar 2015 ist das ehemalige Thüringer Landesamt für Verfassungsschutz als Amt für Verfassungsschutz dem Thüringer Ministerium für Inneres und Kommunales (TMIK) angegliedert. Seit diesem Zeitpunkt gilt auch das neue Thüringer Verfassungsschutzgesetz. Als bundesweit einmalige Regelung sieht es nach § 5 Abs. 2 ThürVerfSchG eine Beteiligung des TLfDI bei der erstmaligen Bekanntgabe personenbezogener Daten im Rahmen der Öffentlichkeitsarbeit vor.

8.2 Kontrolle der Antiterrordatei

Die Antiterrordatei (ATD) ist eine Verbunddatei verschiedener Polizei- und Verfassungsschutzbehörden des Bundes und der Länder. Sie erfasst Personen und Objekte, die einen Bezug zum internationalen Terrorismus aufweisen. Das Antiterrordateigesetz (ATDG) sieht gemäß § 10 Abs. 1 ATDG vor, dass die Kontrolle der Durchführung des Datenschutzes der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) obliegt. Die datenschutzrechtliche Kontrolle der Eingabe und der Abfrage von Daten durch eine Landesbehörde richtet sich nach dem Datenschutzgesetz des Landes. Dementsprechend ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) für die Kontrolle der Thüringer Sicherheitsbehörden in Hinblick auf die ATD zuständig.
Bezüglich der Eingaben und Abfragen in der Antiterrordatei führte der TLfDI im Berichtszeitraum gem. § 37 Thüringer Datenschutzgesetz (ThürDSG) eine datenschutzrechtliche Kontrolle durch. Das Bundesverfassungsgericht hat in seinem Urteil vom 24. April 2013 (BVerfGE -1 BvR 1215/07-) zur Antiterrordatei bereits festgestellt, dass der Gewährleistung einer effektiven Kontrolle eine große Bedeutung zukommt und Zugriffe und Änderungen des Datenbestandes

vollständig zu protokollieren sind (BVerfG Urteil vom 24. April 2013 -1 BvR 1215/07-, Rn. 214f. siehe juris). Dabei muss nach der Aussage des Bundesverfassungsgerichts „durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält“ (BVerfG a.a.O, Rn. 215).
Die Kontrollen der ATD beim Thüringer Landeskriminalamt (TLKA) ergaben bisher keine datenschutzrechtlichen Verstöße, zumal der Datei dort in der Praxis eine eher geringe Bedeutung beigemessen wird. So gab es zum Beispiel keine Suchanfragen in der ATD, die das TLKA im Kontrollzeitraum vorgenommen hätte. In Umsetzung des Urteils des Bundesverfassungsgerichts vom 24. April 2013 wurden auch alle Kontaktpersonen aus der ATD gelöscht. Weitere Nachfragen zu einzelnen Objektkategorien konnten vom TLKA beantwortete werden.
Auch beim Amt für Verfassungsschutz kontrollierte der TLfDI im Berichtszeitraum den Einsatz der ATD und die Protokollierung getätigter Abfragen. Hinweise auf eine rechtswidrige Datenerhebung oder -verarbeitung stellte der TLfDI dabei nicht fest.

§ 10 Abs. 2 ATDG sieht vor, dass die jeweiligen Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer Zuständigkeiten verpflichtet sind, mindestens alle zwei Jahre die Durchführung des Datenschutzes bei der Antiterrordatei zu kontrollieren. Diese regelmäßigen Kontrollen wird auch der TLfDI weiter durchführen.

Datenschutz (Anwalt, Datenschutzbeauftragter) – © fotodo / Fotolia.com

9 Finanzwesen

9.1 Auf Bewährtes vertrauen – keine Geburtsdaten in Kontendaten nutzen

Der Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder diskutierte im Berichtszeitraum Überlegungen eines Finanzministeriums eines anderen Bundeslandes, künftig Zahlungen und Forderungen nicht mehr anhand des Kassenzeichens zu führen, sondern den Betroffenen anhand der Geburtsdaten zuzuordnen, also letztendlich Personenkonten zu führen. Nur so könne eine eindeutige Zuordnung der Personen gewährleistet werden, von denen keine gültigen Adressen vorliegen würden, weil z. B. jemand mehrmals umgezogen sei.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist der Auffassung, dass das Erheben der Geburtsdaten zu o. g. Zwecken datenschutzrechtlich nicht zulässig ist, da Daten gespeichert werden, die nur in ganz bestimmten Fällen erforderlich sein können, um bei der Forderungseintreibung Personenverwechslungen zu vermeiden.

Der TLfDI bat daraufhin das Thüringer Finanzministerium (TFM) mitzuteilen, wie die Thüringer Finanzverwaltung derzeit Zahlungen und Forderungen den betroffenen Personen zuordnet und ob eine Umstellung zu Personenkonten erfolgen solle.
Das TFM teilte dem TLfDI mit, dass im Mittelbewirtschaftungsverfahren „HAMASYS“(=Haushaltsmanagementsystem) die Zuordnung der Zahlungen und Forderungen über das jeweilige Kassenzeichen erfolge. Die Speicherung der Geburtsdaten sei mit Eingabe der Grunddaten nicht vorgesehen. Hier würden lediglich die Adressdaten und die Bankverbindung erfasst.
Die Finanzkassen der Finanzämter ordneten Steuerzahlungen anhand des angegebenen Verwendungszwecks der Überweisung zu. Hier sei das Zuordnungskriterium die Steuernummer, nicht jedoch das Kassenzeichen. Eine maschinelle Zuordnung von Zahlungen zugunsten des Steuerkontos sei nur möglich, wenn Zahlungen zugunsten bestimmter Bankverbindungen geleistet würden und der Steuerpflichtige den korrekten Verwendungszweck, die Kundenreferenznummer, die auf dem Zahlschein enthalten ist, die Steuernummer und ggf. weitere Kriterien angebe. Könne eine maschinelle Zuordnung nicht erfolgen, sei die Einzahlung personell durch den Buchhalter anzuweisen.
Abschließend teilte das TFM mit, dass es nicht vorhabe, das bisherige Zuordnungsverfahren zu ändern.

Der fachliche Austausch im Arbeitskreis Steuerverwaltung ermöglicht es dem TLfDI, seine „Wächterfunktion“ gegenüber der Finanzverwaltung wahrzunehmen und bedenklichen Entwicklungen vorzubeugen, bevor sie sich auf seinen Aufgabenbereich auswirken können. Im Fall der „Zahlungszuordnung per Geburtsdatum“ war – zumindest in Thüringen – „falscher Alarm“ angezeigt, weil auch das TFM die Nachteile einer solchen Umstellung selbst erkannt hatte.

9.2 Neugier auf Kontodaten von Kollegen

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Berichtszeitraum eine Neuregelung zum Zugriff auf Mitarbeiterkontendaten innerhalb einer Sparkasse zu bewerten.
Danach war beabsichtigt, den Mitarbeitern das Recht zu geben, auf Antrag und unter Hinzuziehung des internen Datenschutzbeauftrag-

ten und eines Personalratsmitglieds prüfen zu lassen, ob intern ggf. unberechtigt auf die Kontodaten von Kollegen zugegriffen wurde. Sofern ein unberechtigter Zugriff festgestellt würde, sollte der betroffene Mitarbeiter jedoch nicht den Namen des Kollegen, der zugegriffen hat, erfahren.
Hierzu teilte der TLfDI mit, dass die Mitarbeiter einer Sparkasse ausschließlich im Rahmen ihrer dienstlichen Tätigkeit auf die Kontodaten der Kunden zugreifen dürfen. Eine darüber hinausgehende Nutzung der EDV-Systeme ist nicht erlaubt. Sämtliche Zugriffe auf Kundendaten werden 180 Tage protokolliert. Diese Regelung gilt auch für die Konten eigener Mittarbeiter, d. h. „ein Blick auf das Konto des Kollegen“ ist nur aus dienstlichen Gründen erlaubt.
Der TLfDI sah die Neuregelung zur Kontrolle unberechtigter Zugriffe grundsätzlich als zulässig an. Eine andere Bewertung ergibt sich aus der Sicht des TLfDI dann, wenn grundsätzlich vorgesehen ist, den Namen des Kollegen, der unberechtigt auf ein Konto zugegriffen hat, dem Betroffenen zu offenbaren. Jedoch sind ausnahmsweise Fallkonstellationen denkbar, in denen dem betroffenen Kontoinhaber mitgeteilt werden kann, wer unberechtigt auf sein Konto zugegriffen hat. Hat der Kontoinhaber beispielsweise einen Schaden erlitten, muss er auch die Möglichkeit haben, gegen den Verursacher vorgehen zu können.

Die Schaffung neuer Möglichkeiten zur Feststellung etwaiger unberechtigter Zugriffe auf sensible personenbezogene Daten, wie z. B. Kontendaten und Gesundheits- und Sozialdaten, ist als eine wünschenswerte Missbrauchsprophylaxe anzusehen. Allerdings sind der Ablauf des Kontrollverfahrens und die damit zusammenhängenden personellen Verantwortlichkeiten im Rahmen datenschutzkonformer technisch-organisatorischer Regelungen schriftlich zu fixieren.

9.3 Wenn der Bankautomat spricht

Eine Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) thematisierte Datenschutzaspekte bei der Einführung behindertenspezifischer Identifizierungsmethoden für barrierefreie Bankautomaten.
Im Rahmen der Erarbeitung eines deutschlandweiten Branchenstandards für barrierefreie Bankautomaten sollten unter Mitwirkung des Bundeskompetenzzentrums Barrierefreiheit, der Behindertenverbän-

de und der Deutschen Kreditwirtschaft zusätzliche Identifizierungsmethoden entwickelt werden, die behindertenspezifische Gegebenheiten berücksichtigen. Konkret war beabsichtigt, z. B. auf EC-, VISA- oder Mastercard-Karten personenbezogene Daten zu Menschen mit Behinderungen aufzunehmen. Aufgrund dieser Daten sollten dann am künftigen barrierefreien Bankautomaten bestimmte Voreinstellungen aktiviert werden. Konkret handelte es sich dabei z. B. um Kennzeichen für Blinde und Menschen ohne Hand (Ohnhänder). Sind diese Kennzeichen aktiviert und werden vom Kartenleser erkannt, muss eine Sprachausgabe gewährleistet sein bzw. durch spezifische Technikgestaltung die Entnahme des Geldes aus dem Ausgabeschacht auch für Ohnhänder problemlos möglich sein.
Der TLfDI regte in diesem Zusammenhang an, eine Liste mit solchen spezifischen Daten, die auf der Karte hinterlegt werden können, zu erstellen. Vor der erstmaligen Nutzung sollte der Betroffene jedoch die Möglichkeit erhalten, eine oder mehrere dieser (Listen-) Daten nach einer individuellen Beantragung von der Bank freischalten zulassen.
Da die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 BDSG), sollte die Beantragung solcher Kennzeichen mit einer datenschutzrechtlichen Einwilligung im Sinne von § 4a BDSG verbunden sein. Nach § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG. Personenbezogene Daten nach § 3 Abs. 9 BDSG sind auch Angaben über die Gesundheit des Betroffenen, im konkreten Fall also auch die Daten zu Behinderungen.

Der TLfDI regte an, eine standardisierte Einwilligungserklärung als organisatorische Vorgabe im Rahmen der Schaffung deutschlandweiter Normen für barrierefreie Bankautomaten zu erarbeiten.

Am Beispiel barrierefreier Bankautomaten zeigt sich wieder einmal, wie sinnvoll es ist, frühzeitig datenschutzrechtliche Gesichtspunkte bei der Gestaltung der Technik und von Organisationslösungen zu berücksichtigen. Damit wird dem Grundsatz „Privacy-by-Design" Rechnung getragen. Dieser beinhaltet, dass etwaige Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen sind, sodass der Datenschutz von vornherein in die Gesamtkonzeption einzubeziehen ist.

9.4 Videoüberwachung in Sparkassen –kein Videogaga

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte im Berichtszeitraum aufgrund einer Beschwerde die Videoüberwachung einer Zweigstelle der Sparkasse Mittelthüringen. Konkret war zu klären, wie lange die Bildaufnahmen der Überwachungskamera in den Geldautomaten aufbewahrt werden dürfen und ob die Videoüberwachung des Servicepoints zulässig war.
Vor Ort stellte der TLfDI fest, dass die Überwachungskamera in den Geldautomaten bei jeder Nutzung den Automatennutzer fotografierte. Die Fotos wurden 91 Tage aufbewahrt. Da nach 90 Tagen der Rechnungsabschluss der Konten erfolgte, bestand aufgrund der 91-tägigen Speicherdauer dieser Aufnahmen bei Reklamationen eines Kunden die Chance, eine missbräuchliche Kartennutzung nachzuweisen. Die lange Speicherfrist war und ist auch in Fällen des Skimming – hier schöpft der Täter illegal Daten (z. B. die PIN) von Geld- oder Kreditkarten ab – erforderlich, da hierbei zunächst die Kartendaten illegal im Inland beschafft und dann meist erheblich später in einem niedrigeren ausländischen Kontrollumfeld unbefugt genutzt werden. Die in dem Geldautomaten angefertigten Bilder gab die Sparkasse nur auf Anforderung der Staatsanwaltschaft heraus. Die Kameras im Bereich des Servicepoints waren auf den jeweiligen Kunden bzw. „potentiellen" Täter fokussiert, wobei der zeitweise hinter dem Tresen stehende Mitarbeiter nur peripher abgebildet wurde. Diese Videoaufnahmen speicherte die Sparkasse für die Dauer eines Tages, wobei nur ein kleiner Kreis zuständiger Mitarbeiter

darauf zugreifen durfte. Schriftliche Regelungen zum Umgang mit den Videoaufnahmen lagen nicht vor.
Da es sich bei Sparkassen um öffentliche Stellen handelt, die am Wettbewerb teilnehmen, ist hier nach § 26 Thüringer Datenschutzgesetz (ThürDSG) für die Zulässigkeit von Videoüberwachungen § 6b Bundesdatenschutzgesetz (BDSG) maßgeblich. Zur Feststellung von Überfällen, Betrug und Vandalismus und zur vorbeugenden Abschreckung ist die Videoüberwachung in einer Sparkassenfiliale grundsätzlich gemäß § 6b Abs. 1 Nr. 2 BDSG zulässig, sofern sie erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Da die Kamera zur Überwachung des Servicepoints auf den jeweiligen Kunden bzw. „potentiellen" Täter fokussiert war und der hinter dem Tresen stehende Mitarbeiter nur peripher abgebildet wurde, ging der TLfDI nur von einem geringfügigen Eingriff in das informationelle Selbstbestimmungsrecht der dort zeitweise tätigen Sparkassenmitarbeiter aus. Der Besucher der Sparkasse konnte sich nicht der Videoüberwachung und -aufzeichnung entziehen. Angesichts der Überwachungszwecke und vor dem Hintergrund des bestehenden Gefährdungspotentials sowie der geringen Speicherdauer von einem Tag war es aus der Sicht des TLfDI für den Betroffenen noch akzeptabel, den mit den Aufnahmen verbundenen Eingriff in sein Recht auf informationelle Selbstbestimmung hinzunehmen. Die 91-tägige Speicherdauer der Fotos der Kameras der Geldautomaten war aus Gründen der Aufklärung von Kartenmissbrauch bzw. Betrug erforderlich. Die vorgefundenen Hinweise zur Videoüberwachung entsprachen § 6b Abs. 2 BDSG, wonach der Umstand der Videobeobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Der TLfDI wies die Sparkasse ferner auf das Erfordernis schriftlicher Regelungen zum Umgang mit Videoaufnahmen hin. Im Ergebnis war angesichts des hohen Gefährdungspotentials durch Überfälle eine Videoüberwachung der Sparkassenfiliale mittels Aufzeichnung grundsätzlich als zulässig anzusehen. Dies galt auch für die Speicherdauer der Fotoaufnahmen der Kameras in den Geldautomaten aus Gründen der Betrugsaufklärung. Im Nachgang kam die Sparkasse Mittelthüringen der Forderung des TLfDI nach und legte datenschutzkonforme schriftliche Regelungen zum Umgang mit der Videotechnik vor.

Für Sparkassen als öffentliche Stellen, die am Wettbewerb teilnehmen, gilt gemäß § 26 ThürDSG für den Einsatz von Videoüberwachung § 6b BDSG. Zur Feststellung von Überfällen, Betrug und Vandalismus und zur vorbeugenden Abschreckung ist die Videoüberwachung in einer Sparkassenfiliale grundsätzlich gemäß § 6b Abs. 1 Nr. 2 BDSG zulässig. Jedoch sind im Falle einer Videoüberwachung transparente, unternehmensinterne Regelungen zum Umgang mit der Technik und zu den dafür verantwortlichen Personen in Schriftform erforderlich.

9.5 Datenschutz im Falle einer Gesamtrechtsnachfolge

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Bekanntgabe seiner steuerlichen Daten aus einem Einkommenssteuerbescheid an die Miterben seines verstorbenen Ehepartners. Konkret hatte das Finanzamt den Antrag des Beschwerdeführers, seine Einkünfte auf dem gemeinsamen Einkommenssteuerbescheid der Ehepartner für Zwecke der Bekanntgabe an Miterben seines Ehepartners unkenntlich zu machen, abgelehnt. Durch die Schwärzung wollte der Beschwerdeführer die Weitergabe seiner Einkünfte an die Miterben verhindern.
Das Finanzamt teilte dem TLfDI zu der Beschwerde mit, dass der Beschwerdeführer und die übrigen Erben des Verstorbenen für die Leistungen aus dem Steuerschuldverhältnis Gesamtschuldner nach § 44 Abgabenordung (AO) seien. In den Fällen einer Erbfolge nach § 1922 Abs. 1 Bürgerliches Gesetzbuch (BGB) liege eine Gesamtrechtsnachfolge im Sinne von § 45 AO vor. Forderungen und Schulden gingen kraft Gesetzes auf die Rechtsnachfolger über. Es sei grundsätzlich ein zusammengefasster Bescheid zu erlassen, der an die Gesamtrechtsnachfolger als Gesamtschuldner zu richten und jedem von ihnen bekannt zu geben sei (Pkt. 2.12.3 Anwendungserlass zur AO zu § 122 AO). Es bestehe aber die Möglichkeit, einen Verwaltungsakt an einen Beteiligten mit Wirkung für die anderen Beteiligten bekanntzugeben, soweit alle Beteiligten damit einverstanden seien; die Beteiligten könnten aber auch nachträglich eine Abschrift des Verwaltungsakts verlangen (§ 122 Abs. 6 AO). Eine solche Einverständniserklärung aller Beteiligten lag dem Finanzamt jedoch nicht vor. Somit sei nach der Festsetzung der Einkommens-

teuer der Einkommensteuerbescheid den einzelnen Beteiligten bekannt zu geben (§ 122 AO).
Im Ergebnis stellte der TLfDI fest, dass in diesem Falle die einschlägigen Vorschriften des Steuerrechts eingehalten wurden und kein datenschutzrechtlicher Verstoß vorlag. Eine Bekanntgabe des Steuerbescheides ist dafür erforderlich, dass alle Beteiligten die Zusammensetzung bzw. das Zustandekommen des resultierenden Steuerbetrags nachvollziehen und damit ihre Rechte im Steuerverfahren wahren können.

Die Komplexität datenschutzrechtlicher Sachverhalte zeigt sich insbesondere dann, wenn spezialgesetzliche Vorschriften, in diesem Falle steuerrechtliche Normen, beurteilungsrelevant sind.
In obiger Beschwerdeangelegenheit überwog das Informationsinteresse der Gesamtschuldner zur Wahrung ihrer Rechte aus dem Erbfall das Recht eines Miterben an der Geheimhaltung seines steuerrelevanten Einkommens.

9.6 Besondere Leistungskontrolle in der Thüringer Landesfinanzdirektion

Mehrere Betroffene wiesen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darauf hin, dass in der Thüringer Landesfinanzdirektion (LFD) für einzelne Beamte und Arbeitnehmer die tatsächliche Zahl der Erledigungen erhoben und Zielvorgaben gegenübergestellt und in Listen für den einzelnen Beschäftigten zusammengefasst würden. In einer Dienstversammlung sei sinngemäß verkündet worden, dass „konkrete Maßnahmen zur Sicherstellung des politischen Abarbeitungsziels anlaufen werden“. In den erwähnten Listen sollten von dem jeweiligen Beschäftigten die erledigten Fälle ab dem 1. Februar 2014 alle 14 Tage selbstständig eingetragen werden. Konkrete Bestimmungen, vor allem dazu, wie mit den Listen weiter verfahren werde und zu welchem konkreten Zweck sie genutzt würden, lägen nicht vor. Die Betroffenen befürchteten eine vollständige Leistungs- und Verhaltenskontrolle.
Auf Nachfrage des TLfDI erläuterte die LFD, der Sachverhalt betreffe zwei zum Jahresbeginn 2012 eingegliederte Referate mit derzeit noch etwa 100 Beschäftigten. Bis 2016 sei ein Stellenabbau wegen Erledigung und damit künftigen Wegfalls der Aufgaben auf

zehn Stellen zum Zweck der Restaufgabenerledigung vorgesehen. Bis Ende 2013 sei eine statistische Auswertung der Erledigungen der einzelnen Aufgaben ohne Personenbezug erfolgt. Hierfür habe man die Fachverfahren genutzt. Da aber im Jahr 2013 festgestellt wurde, dass weniger Fälle als in den Vorjahren abgearbeitet wurden, seien die Mitarbeiter der betreffenden Referate in Erwartung eines entsprechenden Erlasses des Thüringer Finanzministeriums informiert worden, dass die Erledigungstermine zwingend einzuhalten seien. Die bisherige Auswertung erachtete man nicht mehr für zielführend und ging dazu über, allen Beschäftigten konkrete Aufgaben zu stellen und die personenbezogene Erledigung durch sie aufzeichnen zu lassen. Weder die Betroffenen noch der Personalrat hätten Bedenken geäußert. Also habe man den Mitarbeitern Vordrucke für handschriftliche Aufzeichnungen zur Erledigung der konkreten Fälle unter Angabe des jeweiligen Stellenzeichens – und damit personenbezogen – ausgehändigt, die monatlich der Referatsleitung zu übergeben waren. Datenschutzrechtliche Bedenken bestehen auch aus Sicht des TLfDI nicht dagegen, dass Fachvorgesetzte personenbezogene Daten zu ihren Mitarbeitern nutzen, soweit dies für die organisatorische und personelle Führung der jeweiligen Organisationseinheit erforderlich ist.

Weiterhin führte die LFD aus, den Mitarbeitern sei auch ein Merkblatt ausgehändigt worden, mit dem im Ergebnis einer internen Prüfung die datenschutzrechtliche Unbedenklichkeit erläutert worden sei. Nach den den Mitarbeitern zur Verfügung gestellten Erläuterungen wurde die Datenerhebung seitens der LFD auf die § 4 Abs. 1 i. V. m. § 19 Abs. 1 ThürDSG gestützt. Die personenbezogenen Daten würden demnach ausschließlich vom Fachvorgesetzten für den vorgenannten Zweck erhoben. Eine Speicherung und Übermittlung der erhobenen Daten war nach Auskunft der Behördenleitung nicht vorgesehen.

Offensichtlich erfolgte diese Information an die Beschäftigten jedoch erst, nachdem die Datenerhebung bereits stattgefunden hatte. Zwar bestehen keine datenschutzrechtlichen Bedenken, wenn Fachvorgesetzte personenbezogene Daten zu ihren Mitarbeitern nutzen, soweit dies für die organisatorische und personelle Führung der jeweiligen Organisationseinheit erforderlich ist. Allerdings musste aus Gründen der Transparenz für die Betroffenen auch erkennbar sein, dass nach dem geschilderten Vorgehen die ausgefüllten Listen das Referat nicht verlassen. Weiterhin musste erkennbar sein, dass die Listen

nach der Auswertung des Bearbeitungsstandes für die weitere Aufgabenerfüllung nicht mehr erforderlich sind und somit einer Löschung unterfallen. Hierauf wurden die Beschäftigten im Nachgang nochmals hingewiesen.

Eine vollständige Leistungs- und Verhaltenskontrolle der Mitarbeiter ist grundsätzlich unzulässig. Eine Kontrolle der Aufgabenerledigung zum Zweck der organisatorischen und personellen Führung durch Fachvorgesetzte, insbesondere einer vor der Umstrukturierung bzw. Auflösung stehenden Organisationseinheit ist jedoch zulässig. Aus Gründen der Transparenz müssen die Betroffenen vor der Datenerhebung über den konkreten Zweck und auch darüber informiert sein, dass keine Datenübermittlungen erfolgen und die Daten nach Auswertung gelöscht werden.

9.7 Drittes Gesetz zur Änderung des Thüringer Gesetzes zur Regelung des Kirchensteuerwesens – alles datenschutzrechtlich ok?

Im Januar 2014 legte das Thüringer Finanzministerium (TFM) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) den Entwurf eines Dritten Gesetzes zur Änderung des Thüringer Gesetzes zur Regelung des Kirchensteuerwesens zur Stellungnahme vor.
Nach datenschutzrechtlicher Prüfung des Gesetzentwurfs teilte der TLfDI dem TFM mit, dass aufgrund der Übereinstimmung der Neuregelung des § 8a Abs. 4 Thüringer Kirchensteuergesetz (ThürKiStG) mit den entsprechenden bundesgesetzlichen Regelungen in § 51a Abs. 2c Einkommensteuergesetz (EStG) die beabsichtigte Gesetzesänderung keinen datenschutzrechtlichen Bedenken begegne. Zugleich regte der TLfDI jedoch an, die im Gesetzentwurf vorgesehene Regelung zu streichen, wonach die Kirchensteuerdaten für andere Zwecke nur dann verwendet werden dürften, soweit der Kirchensteuerpflichtige zustimmt oder dies gesetzlich zugelassen ist. Diese Anregung zielte darauf ab, die Nutzung der sensiblen personenbezogenen Daten zur Zugehörigkeit bzw. Nichtzugehörigkeit der betroffenen Steuerpflichtigen zu einer Religionsgemeinschaft ausschließlich auf den Kirchensteuerabzug zu beschränken.
Bereits bei der Diskussion zur Neuregelung des Einkommensteuergesetzes zur Abführung der Kirchensteuer hatten es die

Datenschutzbeauftragten des Bundes und der Länder als problematisch angesehen, dass das o. g. personenbezogene Datum gegenüber den zum Kirchensteuerabzug verpflichteten Banken und Kreditinstituten zu offenbaren ist. Einen geeigneten Bewertungsmaßstab stellt in diesem Zusammenhang § 28 Abs. 2 Bundesdatenschutzgesetz dar. Danach ist eine zweckändernde Nutzung personenbezogener Daten nur unter den dort genannten engen, im konkreten Falle der Kirchensteuerdaten wohl nicht vorliegenden Voraussetzungen zulässig.
Mit der Neuregelung des Thüringer Kirchensteuergesetzes hätte sich nach Auffassung des TLfDI daher die Gelegenheit geboten, datenschutzrechtlichen Belangen hinsichtlich einer Nutzungsbeschränkung der zum Zwecke der Durchführung des Kirchensteuerabzugs erlangten personenbezogenen Daten seitens der Kirchensteuerabzugsverpflichteten Rechnung zu tragen und keine Begehrlichkeiten zu diesen Daten zu wecken.
Letztendlich ist das TFM der Anregung des TLfDI, die besagte Regelung zur Nutzung von Kirchensteuerdaten für andere Zwecke aus dem Gesetzentwurf zu streichen, nicht gefolgt. Das TFM hielt den Vorschlag des TLfDI für nicht geboten und verwies dabei unter anderem auf § 51a Abs. 2c Satz 9 EStG: Danach darf der Kirchensteuerabzugsverpflichtete die von ihm für die Durchführung des Kirchensteuerabzugs erhobenen Daten ausschließlich für diesen Zweck verwenden.

Kirchensteuerdaten sind als besonders schutzwürdige personenbezogene Daten anzusehen, da aus ihnen religiöse Überzeugungen hervorgehen. Auch wenn der TLfDI nicht für die datenschutzrechtliche Kontrolle der Kirchen und der bei ihnen verarbeiteten personenbezogenen Daten zuständig ist, wird er sich jedoch auch zukünftig im Rahmen der parlamentarischen Anhörungsverfahren zu Gesetzgebungsvorhaben dafür einsetzen, dass Kirchensteuerdaten besonders schutzwürdig bleiben.

paragraph_regen – © fotomek/ Fotolia.com

10 Justiz

10.1 Mitnahme von Gerichtsakten? Datenschutz trotz gesetzlich beschränkter TLfDI-Kontrolle

Ein Beschwerdeführer wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI)

und beschwerte sich darüber, dass der Direktor eines Thüringer Gerichts in einem Zeitungsartikel Ende Januar 2015 Angaben über ein Verfahren gemacht habe, welches nach Auffassung des Beschwerdeführers noch gar nicht rechtskräftig hätte sein können. Zudem habe der Direktor seiner Ansicht nach nicht die Befugnis gehabt, gegenüber der Presse nicht-öffentliche Verfahren zu erörtern. Der TLfDI prüfte den Zeitungsartikel, konnte aber keinen Verstoß gegen datenschutzrechtliche Vorschriften feststellen. Zwar enthielt der Zeitungsartikel Angaben über Verfahren bei dem betreffenden Gericht. Aus diesen Angaben konnte aber aus datenschutzrechtlicher Sicht nicht auf eine konkrete Person geschlossen werden.
In seiner Beschwerde teilte der Beschwerdeführer zudem Folgendes mit: Er wisse, dass Mitarbeiter des Gerichts regelmäßig Gerichtsakten und sonstige Unterlagen mit nach Hause nehmen würden, um dort Heimarbeit zu erledigen, die sie während ihrer regulären Arbeitszeit nicht schaffen würden. Der TLfDI ging auch diesem Hinweis nach, und bat im Rahmen der Zuständigkeit des TLfDI gemäß § 2 Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) das betroffene Gericht um eine Stellungnahme. Aus dieser Stellungnahme ergab sich, dass eine Heimarbeit von Mitarbeitern/innen, die mit der Wahrnehmung von Verwaltungsangelegenheiten betraut sind, nicht durchgeführt wurde. Aus diesem Grund gab es bei dem entsprechenden Gericht bislang auch noch nicht die Notwendigkeit, den datenschutzkonformen Umgang mit Verwaltungsakten bei Heimarbeit zu regeln. Ein Datenschutzverstoß lag demnach nicht vor. Die Kontrollkompetenz des TLfDI für Gerichte bewegt sich dabei im Rahmen des § 2 Abs. 6 ThürDSG und beschränkt sich nur auf deren Verwaltungsangelegenheiten. Das betreffende Gericht bat darum, Hinweise zu geben, falls dem TLfDI Kenntnisse für Datenschutzverstöße vorlägen, die sich auf den Bereich der Rechtssprechungstätigkeit bezögen, um diesen dann in eigener Zuständigkeit nachzugehen.

Für Gerichte gilt das Thüringer Datenschutzgesetz nach § 2 Abs. 6 nur eingeschränkt: Der § 10 (Verfahrensverzeichnis) und der § 11 (Anrufung des Landesbeauftragten für den Datenschutz) sowie der fünfte Abschnitt (Überwachung des Datenschutzes bei öffentlichen Stellen) gelten nur, soweit die Gerichte in Verwaltungsangelegenheiten tätig werden. Das bedeutet aber nicht, dass das Gericht ein datenschutzfreier Raum ist. Auch im Gericht muss der Schutz personenbezogener Daten gewährleistet werden; das heißt, personenbezogene

Daten dürfen grundsätzlich nur verarbeitet werden, wenn eine Rechtsvorschrift dies vorsieht oder eine Einwilligung vorliegt. Im Rahmen einer Veranstaltung mit dem Thüringer Verein der Verwaltungsrichterinnen und Verwaltungsrichter hielt der TLfDI im Sommer 2014 am Verwaltungsgericht Weimar einen Vortrag über den Datenschutz in der Justiz und diskutierte mit den Teilnehmern über einen datenschutzkonformen Umgang mit personenbezogenen Daten im Arbeitsalltag bei Gericht. Eine sehr lebendige Veranstaltung, die vielleicht fortgesetzt werden kann, so die Hoffnung des TLfDI.

10.2 Videoüberwachung oder Zaun? – Was ist bei der Flüchtlingsaufnahmeeinrichtung angemessen?

Im Berichtszeitraum bat das Thüringer Landesverwaltungsamt (TLVwA) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine datenschutzrechtliche Beratung nach § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hinsichtlich einer möglichen Errichtung einer Videoüberwachungsanlage bei einer Außenstelle der Landesaufnahmeeinrichtung für Flüchtlinge. Als Alternative, so das TLVwA, käme auch die Umzäunung der Gebäude in Betracht.
Die datenschutzrechtliche Zulässigkeit einer Videoüberwachung richtet sich bei öffentlichen Stellen nach § 25a Thüringer Datenschutzgesetz (ThürDSG).
Gemäß § 25a Abs. 1 ThürDSG ist eine Videoüberwachung (Videobeobachtung oder -aufzeichnung) zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Unter diesen Voraussetzungen kann eine Videoüberwachung im Gegensatz zu einem Zaun durchaus zulässig sein. Die Erforderlichkeit einer Videoüberwachung ist dann gegeben, wenn das festgelegte Ziel mit der Videoüberwachung tatsächlich erreicht werden kann und dafür kein anderes, gleich wirksames, aber das Recht des Betroffenen weniger beeinträchtigendes Mittel zur Verfügung steht (vgl. für das BDSG: Scholz in Simitis, BDSG Kommentar, § 6b, Rz. 86).
In dem vorgelegten Konzeptentwurf zur Videoüberwachung führte das TLVwA auf, dass eine mögliche Gefährdung durch Personen erfolgen könne, die aufgrund ihrer politischen Einstellung Straftaten gegenüber Personen im Gebäude oder gegen das Gebäude der Au-

ßenstelle der Landesaufnahmestelle für Flüchtlinge zu verüben versuchen würden. Das Gefährdungsrisiko bewertete das TLVwA aufgrund der kontrovers geführten öffentlichen Diskussionen in der Asylthematik als mittel bis hoch. Als Zweck der Videoüberwachung nannte das TLVwA in dem Konzept den Schutz von Leben und Gesundheit der Bewohner der Einrichtung, der Mitarbeiter des Freistaats Thüringen, der Mitarbeiter beteiligter Behörden, von zuständigen Verbänden, Firmen und ehrenamtlichen Helfern, die Gewährleistung der Unversehrtheit und der technischen Funktionstätigkeit der bereitgestellten Einrichtungen sowie der Gebäude, die Abschreckung von möglichen Straftaten und die Möglichkeit zur schnellen Intervention durch die Sicherheitsbehörden.
Der TLfDI wies darauf hin, dass auch der Einsatz milderer Mittel in Betracht zu ziehen sei, wie z. B. die Aufstockung des Sicherheitspersonals, eine bessere Beleuchtung der nicht einsehbaren Bereiche, eine sichere Schließanlage oder ggfs. die Umzäunung des Gebäudes.
Eine weitere Prüfung des TLfDI erübrigte sich, da er im Laufe des weiteren Verfahrens erfuhr, dass die datenschutzkonforme Lösung der Umzäunung der Gebäude gewählt wurde.

Die Zulässigkeit einer Videoüberwachung aus datenschutzrechtlicher Sicht beurteilt sich bei öffentlichen Stellen nach § 25a Thüringer Datenschutzgesetz (ThürDSG).
Gemäß § 25a Abs. 1 ThürDSG ist eine Videoüberwachung (Videobeobachtung oder -aufzeichnung) zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zu prüfen ist insbesondere, ob im Einzelfall nicht mildere Mittel zur Verfügung stehen. Ein milderes Mittel, das das Recht auf informationelle Selbstbestimmung nicht tangiert, kann die Umfriedung/Einzäunung eines Grundstücks sein.

10.3 Datenflüsse an die Staatsanwaltschaft – auf die Rechtsgrundlage kommt es an!

Im Berichtszeitraum bat ein Landratsamt den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine datenschutzrechtliche Prüfung der Weitergabe von Daten der Führerscheinstelle an die Strafverfolgungsbehörde. Hintergrund

war, dass manchen Mitarbeitern der Fahrerlaubnisbehörde bei einer Mitteilung der Strafverfolgungsbehörden nach Nr. 45 (Fahrerlaubnissachen) der Anordnung über Mitteilung in Strafsachen (MiStra) in einzelnen Fällen bekannt sei, dass es sich bei den Personen um Bedienstete des öffentlichen Dienstes handeln würde. Es stand deshalb die Frage im Raum, ob die Mitarbeiter der Fahrerlaubnisbehörde die mitteilende Strafverfolgungsbehörde darüber in Kenntnis setzen dürfen, dass es sich bei den betroffenen Personen um Bedienstete des öffentlichen Dienstes handelt und dass sie deren Dienststelle benennen und auf Nr. 15 und Nr. 16 MiStra hinweisen. Die Nr. 15 und Nr. 16 MiStra regeln, welche Daten in Strafsachen gegen eine Person in einem Beamten- oder Richterverhältnis bzw. gegen Personen in einem Arbeitnehmer- oder sonstigen Beschäftigungsverhältnis im öffentlichen Dienst durch die Staatsanwaltschaft oder das Gericht zu übermitteln sind.
Der TLfDI teilte dem Landratsamt mit, dass die MiStra in ihrem Anwendungsbereich grundsätzlich für die Übermittlung personenbezogener Daten von Amts wegen durch Gerichte und Staatsanwaltschaften an öffentliche Stellen für andere Zwecke als die des Strafverfahrens (für die die Daten erhoben worden sind) gilt (§ 12 ff. Einführungsgesetz zum Gerichtsverfassungsgesetz [EGGVG], Nr. 1, Nr. 4 MiStra). Damit ist es eben nicht Aufgabe der Fahrerlaubnisbehörde, Mitteilungen nach Nr. 15 und Nr. 16 MiStra an die Staatsanwaltschaft zu machen. Eine Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nach § 21 Thüringer Datenschutzgesetz (ThürDSG) zudem nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten liegenden Aufgabe erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Die Fahrerlaubnisbehörde ist jedoch nicht als Strafverfolgungsbehörde tätig und damit auch nicht zuständig für die Verfolgung etwaiger Straftaten. Auch scheint eine Übermittlung an Dritte (hier: die Staatsanwaltschaft) für die Erfüllung ihrer Aufgaben nicht erforderlich zu sein, da die Staatsanwaltschaft eigenständige Ermittlungen durchführt. Eine Datenübermittlung schied in diesem Fall folglich aus. Dies teilte der TLfDI dem Landratsamt mit.

Die Übermittlung personenbezogener Daten stellt auch eine Form der Datenverarbeitung gemäß § 3 Abs. 3 ThürDSG dar. Zur Mitteilung personenbezogener Daten von Amts wegen an öffentliche Stel-

len für andere Zwecke als die des Strafverfahrens sind nach der MiStra bei Strafsachen gegen Personen in einem Beamten- oder Richterverhältnis bzw. gegen Personen in einem Arbeitnehmer- oder sonstigen Beschäftigungsverhältnis grundsätzlich nur die Gerichte und Staatsanwaltschaften nach der gesetzlichen Regelung im Zweiten Abschnitt (§§ 12 ff.) EGGVG befugt. Umgekehrt kann eine Mitteilung durch Mitarbeiter der Fahrerlaubnisbehörde an die Staatsanwaltschaft auf der Grundlage der MiStra nicht vorgenommen werden.

10.4 Dienstlich oder privat – falscher Adressat; wendet sich jemand als Privater an eine öffentliche Stelle, muss an die Privatadresse geantwortet werden

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um eine datenschutzrechtliche Prüfung. Hintergrund war, dass der Beschwerdeführer vor ca. einem Jahr unter Angabe seiner privaten Daten bei einer Thüringer Polizeiinspektion Anzeige gegen Unbekannt wegen Sachbeschädigung erstattet hatte. Nun habe er einen Bescheid der Staatsanwaltschaft Erfurt erhalten mit der Mitteilung, dass die Ermittlungen ergebnislos verlaufen seien. Die Staatsanwaltschaft habe daher das Verfahren eingestellt. Diesen Brief habe die Staatsanwaltschaft aber nicht an die Privatadresse des Beschwerdeführers, die er bei der Anzeigeerstattung angeben hatte, sondern an seine Dienststelle versandt. Der Brief enthielt zudem keinen zusätzlichen Vermerk wie „persönlich“ oder „vertraulich“.
Der TLfDI wandte sich an die Staatsanwaltschaft Erfurt und bat sie um eine Stellungnahme.
Aus dieser ging hervor, dass der Beschwerdeführer bereits vor fast drei Jahren zunächst in seiner dienstlichen Funktion Strafanzeige wegen Sachbeschädigung erstattet hatte. Dabei übernahm die Staatsanwaltschaft die dienstlichen Daten in der Strafanzeige und erfasste sie elektronisch. Das Ermittlungsverfahren wurde eingestellt. Zwei Jahre später erstattete der Beschwerdeführer – nun als Privatperson – erneut eine Anzeige wegen Sachbeschädigung. In diesem Ermittlungsverfahren nahm die Staatsanwaltschaft dieses Mal die Privatanschrift des Beschwerdeführers auf. Auch dieses Verfahren wurde später eingestellt. Den Einstellungsbescheid übersandte die Staats-

anwaltschaft jedoch versehentlich nicht an die Privatanschrift des Beschwerdeführers, sondern an die aus dem vorherigen Verfahren bekannte Dienstanschrift. Die Staatsanwaltschaft wies in ihrer Stellungnahme an den TLfDI auf Folgendes hin: Nach Eingang der Ermittlungsakten erfasse die Staatsanwaltschaft (Zentrale Registerstelle) die Daten der Anzeigeerstatter und der Beschuldigten. Die Daten blieben solange im System der Staatsanwaltschaft, bis sie die gegenständliche Akte entsprechend den Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden vernichten könne. Diese sehen eine Aufbewahrungsfrist von fünf Jahren für Akten über Ermittlungsverfahren vor, welche aus sonstigen Gründen eingestellt wurden. Die Staatsanwaltschaft Erfurt teilte mit, dass sowohl die Dezernenten als auch die Geschäftsstelle bei der Generierung der Schriftstücke prüfen müssten, ob die im System eingepflegten Daten korrekt sind. Dies sei in diesem Fall versehentlich nicht geschehen. Zugleich teilte die Staatsanwaltschaft mit, dass sich die zuständige Abteilungsleiterin anlässlich eines Telefonats mit dem Beschwerdeführer für diesen Fehler entschuldigt habe. Die Staatsanwaltschaft Erfurt nahm den Vorfall zum Anlass, ihre Mitarbeiter auf diese besondere Prüfpflicht nochmals hinzuweisen. Aufgrund dieser umgehenden Reaktion der Staatsanwaltschaft Erfurt sah der TLfDI von einer förmlichen Beanstandung ab.

Um Verwechselungen oder eine falsche Zustellung möglichst zu vermeiden, müssen die öffentlichen Stellen immer genau prüfen, ob die Daten, die sie für ihre Vorgangsbearbeitung nutzen, noch zutreffend sind. Dazu sind gemäß § 9 Thüringer Datenschutzgesetz auch die erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

10.5 Gesetzentwurf zur Aufbewahrung von Notariatsunterlagen – nicht ohne Datenschutz

Im Berichtzeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis, dass ein Gesetzentwurf in Arbeit sei, welcher die Aufbewahrung von Notariatsunterlagen regeln soll. Vorgesehen sei unter anderem die Errichtung eines Elektronischen Urkundenarchivs. Auf Nachfrage des TLfDI beim zuständigen Thüringer Ministerium für Migration,

Justiz und Verbraucherschutz (TMMJV) erhielt er den von einer Länderarbeitsgruppe erarbeiteten Entwurf eines Gesetzes zur Neuordnung der Aufbewahrung von Notariatsunterlagen und Errichtung eines elektronischen Urkundenarchivs bei der Bundesnotarkammer übersandt.

Für kritikwürdig erachtete der TLfDI dabei folgende Punkte:

Nach dem Gesetzentwurf hat „der Notar die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Verschwiegenheit und Datensicherheit zu gewährleisten“. Da aber das Verfahren zentral bereitgestellt wird, kann der Notar die Gewährleistung der Verschwiegenheit und Datensicherheit in Bezug auf das Urkundenarchiv nur bedingt selbst veranlassen. Insofern erschien es dem TLfDI nicht schlüssig, warum allein der Notar uneingeschränkt die entsprechenden Maßnahmen treffen und ggf. verantworten muss.

Das Bundesministerium der Justiz und für Verbraucherschutz soll nach dem Gesetzentwurf durch Rechtsverordnung mit Zustimmung des Bundesrates die näheren Bestimmungen treffen, die für den Schutz jener Daten notwendig sind, die der Verschwiegenheitspflicht des Notars unterliegen. Darunter fallen z. B. die erforderlichen Zutritts-, Zugangs-, Zugriffs-, Weitergabe- und Verfügbarkeitskontrollen.

Der TLfDI empfahl, auch die Eingabekontrolle in diese Aufzählung aufzunehmen, da damit geprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

Nach dem Gesetzentwurf ist der Notar verpflichtet, „Akten und Verzeichnisse so zu führen, dass ihre Verfügbarkeit, Transparenz und Vertraulichkeit gewährleistet ist“.

Da gerade bei elektronischen Akten die Integrität – das heißt, es soll gewährleistet sein, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (vgl. § 9 Abs. 2 Nr. 2 ThürDSG) – eine große Rolle spielt, sollte auch diese im Gesetzentwurf Berücksichtigung finden.

Der Gesetzentwurf sah weiterhin vor, dass das Bundesministerium der Justiz und für Verbraucherschutz Auskunfts- und Einsichtsrechte in einer Rechtsverordnung regeln soll. Das Auskunft- und Einsichtsrecht ist ein wesentlicher Bestandteil des Rechts auf informationelle Selbstbestimmung (vgl. § 13 ThürDSG). Wenn es dazu Beschränkungen in einer Rechtsverordnung geben soll – die nicht grundsätz-

lich ausgeschlossen sind – muss der Rahmen dazu im Gesetz geregelt sein und nicht in einer Rechtsverordnung (Artikel 80 Grundgesetz (GG)).
Nach dem Gesetzentwurf besteht zudem keine Pflicht des Notars oder mehrerer Notare, die sich zur gemeinsamen Berufsausübung verbunden oder gemeinsame Geschäftsräume haben, zur Bestellung eines Datenschutzbeauftragten.
Aus datenschutzrechtlicher Sicht begegnet diese geregelte „Befreiung" der Notare von der Pflicht, einen behördlichen Datenschutzbeauftragten (bDSB) zu bestellen, erheblichen Bedenken. § 10a Abs. 1 Satz 4 ThürDSG legt fest, dass u. a. Notare einen Beauftragten einzusetzen haben, wenn mindestens fünf Personen bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden.
Der Datenschutzbeauftragte ist nicht nur für das elektronische Urkundenarchiv, sondern auch etwa für die Mitarbeiterdaten und andere, nicht originär der Notarstätigkeit zuzuordnende Verfahren (Webseite, Internetzugang, Telefonanlage etc.) zuständig.
Der Gesetzesentwurf sah zudem eine Änderung des § 92 Bundesnotarordnung (BNotO) vor, was aus datenschutzrechtlicher Sicht absolut inakzeptabel wäre. Diese Änderung bezweckte ausweislich der Gesetzesbegründung, die Notare von der Kontrolle durch die Landesbeauftragten für den Datenschutz vollständig auszunehmen. Die Datenschutzkontrolle soll danach in jeder Hinsicht – also auch im Hinblick auf den Datenschutz – nur noch („ausschließlich") durch die in § 92 BNotO genannten Stellen der Justizverwaltung durchgeführt werden. Die dafür genannten Gründe überzeugen – jedenfalls für die in Thüringen geltende Rechtslage – nicht. Notare sind eindeutig und voll umfänglich dem Geltungsbereich des ThürDSG unterworfen (vgl. § 2 Abs. 1 ThürDSG), da sie als Beliehene zu Trägern eines öffentlichen Amtes bestellt werden. Damit unterfallen die Notare in Thüringen auch der Prüfungskompetenz des TLfDI nach § 37 Abs. 1 ThürDSG. Eine differenzierte Behandlung öffentlicher Stellen erscheint nicht sinnvoll und wäre den Betroffenen auch kaum vermittelbar. Im Übrigen erscheint es auch sehr fraglich, ob die beabsichtigte Datenschutzaufsicht ausschließlich durch die in § 92 BNotO genannten Stellen der Justizverwaltung mit den Vorgaben des Art. 28 Abs. 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (EG-Datenschutzrichtlinie) im Einklang steht, wonach die mit der Überwachung des Datenschutzes beauftragte

Stelle ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Die Stellen der Justizverwaltung unterstehen in Ausübung ihrer Funktion des § 92 BNotO jeweils selbst der Dienstaufsicht durch die übergeordneten Organe der Justizverwaltung bzw. letztlich durch den zuständigen Minister. Eine völlige Unabhängigkeit in der Wahrnehmung der Aufgaben der Datenschutzkontrolle ist daher bei diesen nicht gewährleistet (EuGH, Urteil vom 9. März 2010 Az.: C-518/07). Zudem fällt es den von einem Datenschutzverstoß durch einen Notar möglicherweise Betroffenen in vielen Fällen womöglich leichter, sich – statt an ein Organ der Justizverwaltung – an einen Landesdatenschutzbeauftragten zu wenden, der in Ausübung seines Amtes unabhängig ist und dem Betroffenen und seinen Eingaben stets Vertraulichkeit zusichern kann. Schließlich erschließt sich nicht, inwiefern Organe der Justizverwaltungen eine gegenüber den Landesdatenschutzbeauftragten erhöhte „Fachnähe“ besitzen und daher zur Ausübung der Datenschutzaufsicht besser geeignet sein sollen als die Landesdatenschutzbeauftragten.
Ob die datenschutzrechtlichen Bedenken und Hinweise im Rahmen des weiteren Gesetzgebungsverfahrens berücksichtigt werden, behält der TLfDI im Auge.

Kurz und knapp zusammengefasst:
Wesentlicher Kritikpunkt des Gesetzentwurfs zur Aufbewahrung von Notariatsunterlagen ist zum einen die Möglichkeit, Regelungen der Auskunfts- und Einsichtsrechte in einer Rechtsverordnung und nicht in einem Gesetz zu bestimmen. Ferner moniert der TLfDI, dass es keine Verpflichtung geben soll, einen Datenschutzbeauftragten zu bestellen, und dass die Notare nicht mehr der Kontrolle des TLfDI unterliegen sollen.

10.6 Ja, wer lauscht denn da in der JVA!?

Bereits im 10. Tätigkeitsbericht informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Kontrolle einer Thüringer Justizvollzugsanstalt (JVA).
Dabei stellte der TLfDI fest, dass sich unter anderem an den Haftraumtüren unterschiedliche personenbezogene Daten der Gefangenen, wie der Vorname, der Nachname, spezielle Gesundheitsdaten (z. B. Diabetiker), die Religionszugehörigkeit (z. B. Moslem), die speziellen Essgewohnheiten (z. B. muslimische Kost) und der Hin-

weis auf die Arbeitsstätte in der Justizvollzugsanstalt befanden. Dies sah der TLfDI im Hinblick auf die Gesundheitsdaten und die Religionszugehörigkeit kritisch. Auch folgte die JVA dem Rat des TLfDI und verzichtete nunmehr auf die Angabe von Gesundheitsdaten und der Religionszugehörigkeit an den Haftraumtüren.
Weiterhin veranlasste die JVA, dass keine Krankenakten oder personenbezogene Daten von Gefangenen in unverschlossenen Schränken oder sichtbar und frei zugänglich im medizinischen Bereich lagerten.
Darüber hinaus befindet sich in der Vollzugsgeschäftsstelle der JVA ein Ausleihblatt für Archivakten, aus dem ersichtlich ist, wer wann und aus welchem Grund Einsicht in die Gefangenenpersonalakte genommen hat.
Das zwischenzeitlich in Kraft getretene Thüringer Justizvollzugsgesetzbuch (ThürJVollzGB) vom 27. Februar 2014 regelt in § 139 ThürJVollzGB nunmehr auch den Umgang von Gefangenendaten nach deren Entlassung oder einer Verlegung. Danach sind diese Daten spätestens nach Ablauf von zwei Jahren seit der Entlassung oder der Verlegung der Gefangenen in eine andere Anstalt zu kennzeichnen. Ihre weitere Verarbeitung oder Nutzung ist einzuschränken (Sperrung). Die Daten sind nach Ablauf der Frist nur noch ausgewählten Bediensteten zugänglich zu machen. Einzelheiten regelt der Anstaltsleiter. Hiervon können bis zum Ablauf der Aufbewahrungsfrist nach § 140 ThürJVollzGB die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum der Gefangenen ausgenommen werden, soweit dies für das Auffinden der Gefangenenpersonalakte erforderlich ist.
Bei der Aufbewahrung von Akten und Dateien mit nach § 139 ThürJVollzGB gesperrten Daten darf gemäß § 140 ThürJVollzGB für Gefangenenpersonalakten, Gesundheitsakten, Therapieakten, psychologische und pädagogische Testunterlagen und Krankenblätter sowie für Gefangenenbücher eine Frist von dreißig Jahren nicht überschritten werden.
Als wichtigste datenschutzrechtliche Neuregelung betrachtet der TLfDI die Ausgestaltung der Überwachung der Telefonate der Gefangenen.
Dazu vertrat der TLfDI bereits im 10. Tätigkeitsbericht (Nr. 10.1: Datenschutz hinter Gittern – auch in einer Justizvollzugsanstalt gilt das Grundrecht auf informationelle Selbstbestimmung, S. 183 ff.) die Auffassung, dass das informationelle Selbstbestimmungsrecht des Gefangenen und seines Gesprächspartners es erfordern, beide vor

Beginn des Gespräches über die beabsichtigte Überwachung zu informieren (so auch Schwind in: Schwind, Böhm, Jentzle, Laubenthal, StVollzG Kommentar, 6. Auflage 2013, § 32, Rn. 4; Calliess/ Müller-Dietz, Strafvollzugsgesetz Kommentar, 2008, § 32, Rn. 1; Joester/Wegner in: Feest/ Lesting, Strafvollzugsgesetz, Kommentar, 6. Auflage 2012, § 32, Rn. 14). Ein unbemerktes Abhören von Gesprächen ist nicht zulässig (so auch OLG Hamm, Beschluss vom 21. Oktober 2008 – 1 Vollz (Ws) 635/08 Rn. 11 –, zitiert nach der juris-Entscheidung). Eine automatisierte Bandansage, die lediglich auf die Möglichkeit einer Überwachung hinweist, ist mit dem Gesetz somit nicht vereinbar. Die JVA muss daher zwingend bei jedem Gespräch, das tatsächlich überwacht werden soll, von Beginn an mitteilen, dass eine Überwachung stattfindet.

Das damalige Thüringer Justizministerium (TJM) vertrat hingegen die Ansicht, dass die Vollzugsanstalten bundesweit allgemeine Bandansagen einsetzen durften und diese datenschutzrechtlich überprüft seien. Bei der bisher angewandten Verfahrensweise könnte die Forderung des TLfDI nach einem konkreten Hinweis vor Aufnahme des Telefonats nicht umgesetzt werden, weil der Bedienstete der JVA nicht wissen könne, wann der Gefangene mit wem telefoniere. Aus diesem Grund käme laut TJM allenfalls in Betracht, dass im Falle des Zuschaltens des Bediensteten in ein laufendes Telefonat künftig ein konkreter Hinweis auf die Überwachung des Telefonats erfolge. Die technischen Möglichkeiten hätten nach der damaligen Aussage des TJM jedoch erst mit dem Telefonanbieter erörtert werden müssen.

Der TLfDI vertrat jedoch weiterhin die Auffassung, dass eine allgemeine Bandansage vor jedem Telefonat der Mitteilungspflicht des § 38 Abs. 1 S. 3 ThürJVollzGB nicht genüge und somit unzulässig sei. Der Mithörhinweis – so der TLfDI – könne nur in dem Fall einer tatsächlichen Nutzung der Funktion des Mithörens erfolgen.

§ 38 Abs. 1 Satz 3 ThürJVollzGB sieht vor, dass die Anstalt eine beabsichtigte Überwachung den Gefangenen rechtzeitig vor Beginn des Telefongesprächs und den Gesprächspartnern der Gefangenen unmittelbar nach Herstellung der Verbindung mitteilt. Durch den Verweis in § 38 Abs. 1 Satz 2 ThürJVollzGB auf die entsprechende Geltung der Bestimmungen über den Besuch (§§ 34 bis 37 ThürJVollzGB) sind die Telefonate grundsätzlich nicht überwacht. Ein unbemerktes Abhören von Gesprächen ist demnach generell nicht zulässig. Zudem verunsicherte die damalige Verfah-

rensweise alle Telefonierenden (sowohl den Gefangenen als auch den Angerufenen). Irritierend war es darüber hinaus, wenn die Bandansage auch bei Gesprächen zu laufen begann, die an sich schon von der Überwachung ausgenommen sind (z. B. Telefonate des Gefangenen mit seinem Verteidiger). Es hätte sich in diesem Fall die weitergehende Frage gestellt, ob eine Überwachung der Telefonate tatsächlich nicht stattfindet. Eine Nachfrage seitens des TLfDI in den anderen Bundesländern ergab zudem, dass viele Justizvollzugsanstalten seit längerer Zeit gänzlich auf die vorherige Bandansage verzichten. Eine Bandansage bzw. ein Hinweis auf die Überwachung läuft dort nur noch bei tatsächlich abgehörten Gesprächen. Auch vor dem Hintergrund, dass eine Überwachung in der Praxis in Thüringen wohl nur sehr selten vorkommt, hielt der TLfDI die Abschaltung des allgemeinen Hinweises auf eine mögliche Überwachung für angebracht. Muss eine JVA tatsächlich ein Gespräch überwachen, so ist die beabsichtigte Überwachung den Telefonierenden vorab mitzuteilen. Da die Bandansage mit dem allgemeinen Hinweis bei fast allen Thüringer Justizvollzugsanstalten programmiert war, wies der TLfDI darauf hin, auch dort eine entsprechende Änderung der Verfahrensweise vorzunehmen.
Das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) (ehemals Thüringer Justizministerium) folgte schließlich der Rechtsauffassung des TLfDI. Das TMMJV wies die Justizvollzugsanstalten des Freistaates Thüringen an, den Ansagetext der Gefangenentelefonanlagen entsprechend anzupassen, sodass zukünftig nur noch dann ein Hinweis auf eine Überwachung erfolgt, wenn die JVA das Telefongespräch tatsächlich mithört.

Auch Gefangene haben ein Grundrecht auf informationelle Selbstbestimmung. Dieses kann zwar durch ein Gesetz eingeschränkt werden, dessen Tatbestandsmerkmale müssen jedoch vorliegen. So sieht § 38 Abs. 1 S. 3 ThürJVollzGB vor, dass die Anstalt eine beabsichtigte Überwachung den Gefangenen rechtzeitig vor Beginn des Telefongesprächs und den Gesprächspartnern der Gefangenen unmittelbar nach Herstellung der Verbindung mitteilt. Eine allgemeine Bandansage, die möglicherweise auf eine Arbeitserleichterung zurückzuführen ist, die vor jedem Gespräch läuft, ist nicht zulässig.

10.7 Übermittlungssperre für Staatsanwaltschaft

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde eines Bürgers aus Nordrhein-Westfalen, der folgenden Sachverhalt schilderte:
Der Bürger habe Ende des Jahres 2014 per E-Mail eine Strafanzeige gegen den Inhaber einer Firma wegen Betruges gestellt. Da sich aber der Sitz dieser Firma, der Wohnort des beschuldigten Firmeninhabers und damit der Tatort in Jena befänden, habe die bisher zuständige Staatsanwaltschaft aus Nordrhein-Westfalen das geführte Ermittlungsverfahren an die Staatsanwaltschaft Gera abgegeben. Die Staatsanwaltschaft Gera gab sodann im Rahmen der Registrierung des zugrunde liegenden Ermittlungsverfahrens im Fachverfahren websta (das einem speziellen elektronischen Aktenführungssystem nahekommt) die Wohnortadresse und nicht die Postfachadresse des Bürgers und Anzeigeerstatters ein. Grund hierfür war – nach dem späteren glaubhaften Vorbringen der Staatsanwaltschaft Gera gegenüber dem TLfDI –, dass die vom Bürger aus Nordrhein-Westfalen per E-Mail erstattete Strafanzeige ausgedruckt und in der Akte zum Teil verdeckt war. Infolgedessen nahm bei der Staatsanwaltschaft niemand zur Kenntnis, dass der Anzeigenerstatter am Ende seiner E-Mail-Strafanzeige auf die für seine Privatanschrift bestehende Auskunftssperre hinwies. Auch die Bitte des Anzeigenerstatters, dass seine Privatanschrift nicht in die Ermittlungsakte aufgenommen werden sollte, beachtete bei der Staatsanwaltschaft Gera niemand. Schließlich erkannte die Staatsanwaltschaft Gera nicht, dass der Anzeigenerstatter ganz unten links in seiner E-Mail-Strafanzeige seine Postfachadresse in Nordrhein-Westfalen angegeben hatte.
Dieser Lapsus der Staatsanwaltschaft Gera fiel dem Bürger und Anzeigenerstatter aber dann auf, als er im Winter 2015 Post von der Staatsanwaltschaft Gera an seine Privatanschrift erhielt und ihm mitgeteilt wurde, dass das strafrechtliche Ermittlungsverfahren eingestellt worden sei. Da der Bürger und Anzeigenerstatter in Sorge war, dass seine Privatanschrift aus der Akte der Staatsanwaltschaft Gera an Dritte übermittelt worden sein könnte, bat er den TLfDI um Hilfe. Dieser prüfte den Fall und kam zu folgenden Ergebnissen:
Die bei der Staatsanwaltschaft (StA) Gera im Programm websta gespeicherte Wohnortadresse des Bürgers und Anzeigenerstatters war nach § 16 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG)

zu löschen, weil die Kenntnis der Wohnortadresse zur Erfüllung der Aufgaben der StA Gera nicht (mehr) erforderlich war. Dies ergab sich zum einen aus der Tatsache, dass der StA Gera – nach eigenem Bekunden – von vornherein auch die Postfachadresse des Bürgers und Anzeigenerstatters bekannt gewesen sei. Folglich war es demnach auch nicht erforderlich, dass die StA Gera die Wohnortadresse des Bürgers und Anzeigenerstatters ins Programm websta übernahm.
Zum anderen war die im Programm websta gespeicherte Wohnortadresse für die StA Gera nicht mehr erforderlich, weil das bei ihr geführte Ermittlungsverfahren laut Mitteilung der StA Gera an den TLfDI im Winter 2015 eingestellt worden war.
Schließlich war dabei auch die melderechtliche Auskunftssperre zugunsten des Bürgers und Anzeigenerstatters im Sinne von § 34 Abs. 6 Meldegesetz NRW zu berücksichtigen.
Ferner war die Wohnortadresse des Bürgers und Anzeigenerstatters gemäß § 16 Abs. 2 Satz 2 ThürDSG in Verbindung mit § 15 Abs. 1 ThürDSG auch in den Akten der Staatsanwaltschaft Gera zum zugrunde liegenden Ermittlungsverfahren zu sperren. Dies ergab sich daraus, dass die Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaft und der Justizvollzugsbehörden (Aufbewahrungsbestimmungen – AufbewBest – hier Anlage zu Nr. 2 der AufbewBest, laufende Nummer 621 b) bei einer Einstellung eines Ermittlungsverfahrens aus sonstigen Gründen eine Aufbewahrungsfrist für die staatsanwaltschaftliche Ermittlungsakte von fünf Jahren vorsehen. Damit konnten die personenbezogenen Daten – hier in Gestalt der Wohnortadresse des Bürgers und Anzeigenerstatters – in der Ermittlungsakte der StA Gera zwar nicht sofort gelöscht, sehr wohl aber gemäß § 15 Abs. 1 ThürDSG gesperrt werden.
Der TLfDI forderte die Staatsanwaltschaft Gera daher auf, die Wohnortadresse des Bürgers und Anzeigenerstatters als personenbezogenes Datum im Programm websta gemäß § 16 Abs. 1 Nr. 2 ThürDSG zu löschen und die Wohnortadresse als personenbezogenes Datum in der Ermittlungsakte der Staatsanwaltschaft Gera (Az. 390 Js 165/15) gemäß § 16 Abs. 2 Satz 2 in Verbindung mit § 15 Abs. 1 ThürDSG zu sperren.
Ferner mahnte der TLfDI dringend an, den Inhalt von Strafanzeigen, insbesondere darin enthaltene Hinweise auf melderechtliche Übermittlungssperren, künftig effektiver zu beachten und zu berücksichtigen und Strafanzeigen in Papierform dergestalt abzuheften, dass ihr

Inhalt für den Bearbeiter leicht und jederzeit sichtbar zur Kenntnis genommen werden kann.
Die Staatsanwaltschaft Gera teilte dem TLfDI daraufhin mit, dass sie Vorgaben des TLfDI berücksichtigt habe und in zukünftigen Fällen anwenden werde. Der TLfDI sah deshalb von einer Beanstandung gemäß § 39 Abs. 3 ThürDSG ab. Für den Bürger und Anzeigenerstatter besonders wichtig war ferner der Hinweis der Staatsanwaltschaft Gera, dass seine private Wohnanschrift in der Ermittlungsakte von keiner dritten Person eingesehen und damit nicht an Dritte übermittelt worden war. Dies teilte der TLfDI dem Bürger und Anzeigenerstatter abschließend mit.

Auch eine Staatsanwaltschaft hat das Gebot der Datensparsamkeit gemäß § 1 Abs. 2 Satz 1 ThürDSG zu beachten und personenbezogene Daten gemäß § 16 Abs. 1 Nr. 2 ThürDSG zu löschen, wenn diese zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind. Dies gilt erst recht für das personenbezogene Datum der privaten Wohnanschrift eines Anzeigenerstatters, wenn dafür zum einen eine melderechtliche Auskunftssperre besteht und der Staatsanwaltschaft zum anderen eine Postfachadresse des Anzeigenerstatters bekannt ist.

10.8 Anforderung von Ausländerakten zur Anerkennung ausländischer Entscheidungen in Ehesachen

Im Berichtszeitraum hat der Arbeitskreis „Justiz“ der Landesbeauftragten für den Datenschutz die Praxis der Anforderung von Ausländerakten bei Verfahren zur Anerkennung ausländischer Entscheidungen in Ehesachen thematisiert. Die Beiziehung von Ausländerakten in Familiensachen in diesem Zusammenhang geschieht unterschiedlich.
In einem Bundesland werden die Ausländerakten in Familiensachen in diesen Angelegenheiten grundsätzlich beigezogen, in anderen Bundesländern stellt dies die Ausnahme dar.
Nach § 107 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) sind die Justizverwaltungen der Länder für die Anerkennung ausländischer Entscheidungen in Ehesachen zuständig. Das Beiziehen von Ausländerakten betrifft häufig Fälle, in denen ein in Deutschland lebender Ausländer eine neue Ehe (ggf. mit einer/einem Deutschen) eingehen möchte und dafür die verbindliche Bestätigung benötigt,

dass eine frühere Ehe im Ausland inzwischen rechtskräftig geschieden wurde. Die Anerkennung erfolgt auf Antrag.
In Anerkennungsverfahren fordert die zuständige Justizbehörde des Bundeslandes – das zur Nachfrage Anlass gegeben hatte – von der Ausländerbehörde regelmäßig die Ausländerakte der antragstellenden Person an, ggf. auch die des Ex-Ehepartners. Dieser Akte entnimmt die Justizbehörde Angaben für den Antrag oder auch die Bestätigung, dass die von der antragstellenden Person in dem Antragsformular gemachten Angaben zutreffen.
Die Übersendung der gesamten Ausländerakte führt allerdings zur Übermittlung nicht erforderlicher, zum Teil sehr sensibler Daten an eine dritte Stelle.
In Thüringen ist der Präsident des Oberlandesgerichts für die Entscheidungen über Anträge zur Anerkennung ausländischer Entscheidungen in Ehesachen zuständig. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erkundigte sich beim damaligen Thüringer Justizministerium (TJM), wie die Thüringer Familiengerichte die Beiziehung der genannten Ausländerakten handhaben. Nach Auskunft des TJM würden in Thüringen bei Anerkennungsverfahren nach § 107 FamFG Ausländerakten nicht regelmäßig, sondern nur aus besonderem Anlass beigezogen. Dies geschehe insbesondere dann, wenn Zweifel an der Identität des Betroffenen oder an den Angaben zum Familienstand bestünden und daher eine Überprüfung geboten erscheine. Der familienrechtliche Sachverhalt sei von Amts wegen aufzuklären. Das ergibt sich aus § 26 FamFG. Gemäß § 29 FamFG erhebt das Gericht die erforderlichen Beweise in geeigneter Form. Dazu zählt, so das TJM, auch die Einholung amtlicher Auskünfte von Behörden sowie die Einsichtnahme in jede Art von Urkunden, insbesondere auch die Einsicht in Behördenakten. Aus besonderem Anlass könne somit auch die Ausländerakte in das Verfahren einbezogen werden.
Aus Sicht des TLfDI stieß die Thüringer Praxis – die Beiziehung der ausländischen Akte in Anerkennungsverfahren nach § 107 lediglich in begründeten Ausnahmefällen – auf keine Bedenken.

In Ausnahmefällen können Ausländerakten in Familiensachen bei Anerkennungsverfahren beigezogen werden, wenn das Ziel der Informationsgewinnung, insbesondere die Klärung der Personalien und Staatsangehörigkeiten der Beteiligten, Aufenthaltsorte und -dauer,

Nachweis der Eheschließung oder auch der genaue Trennungszeitpunkt auf andere Weise nicht sicher geklärt werden kann.

10.9 Zugang zu Gefangenendaten des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT)

Das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit TLfDI im Berichtszeitraum um eine Stellungnahme hinsichtlich des Zugangs des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT) zu Gefangenendaten. Das CPT besucht Hafteinrichtungen und prüft, wie die Gefangenen dort behandelt werden.
Eine Einsichtnahme des CPT in die Gefangenenpersonalakte und/oder Krankenakte bzw. eine Übermittlung der Daten an den CPT wäre nur zulässig, wenn eine Rechtsgrundlage die Datenverarbeitung erlauben würde oder eine Einwilligung der Betroffenen vorläge (§ 4 Abs. 1 Thüringer Datenschutzgesetz [ThürDSG]).
Art. 8 Abs. 2 d der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe stellte nach der Ansicht des TLfDI keine taugliche Rechtsgrundlage für eine Einsichtnahme der Mitglieder des CPT in die Gefangenenpersonal- und/oder die Gesundheitsakte dar.
Art 8 Abs. 2 d der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung von Strafe bestimmt, dass die Vertragspartei – also auch die Bundesrepublik Deutschland, die der Konvention beigetreten ist – dem CPT alle sonstigen zur Verfügung stehenden Auskünfte, die der CPT zur Erfüllung seiner Aufgabe benötigt, zu gewähren hat. Bei der Beschaffung solcher Auskünfte beachtet der CPT die innerstaatlichen Rechtsvorschriften einschließlich des Standesrechts. In dem „Erläuternden Bericht“ wird dazu ausgeführt, dass der CPT seinerseits verpflichtet ist, die geltenden Regeln der nationalen Rechtsvorschriften und des Standesrechts (insbesondere Regeln bezüglich des Datenschutzes und des Arztgeheimnisses) zu berücksichtigen, wenn er eine Vertragspartei um Auskünfte ersucht. Nach der Auffassung des TLfDI hat die Konvention ausdrücklich einen Vorbehalt in Bezug auf nationale Datenschutzbestimmungen vorgesehen. Eine spezialge-

setzliche Regelung lässt sich aus der Konvention somit nicht ableiten. Auch das Thüringer Justizvollzugsgesetzbuch (ThürJVollzGB), das grundsätzlich als spezialgesetzliche Bestimmung den Regelungen des Thüringer Datenschutzgesetzes vorgeht, sieht keine taugliche Rechtsgrundlage hinsichtlich einer Einsichtnahme bzw. einer Übermittlung der Gefangenendaten sowie Krankendaten an das CPT vor.

§ 119 ThürJVollzGB bestimmt jedoch, dass das Thüringer Datenschutzgesetz (ThürDSG) Anwendung findet, soweit in diesem Gesetz nichts Abweichendes geregelt ist. Das ThürDSG differenziert dabei zwischen der Datenverarbeitung (hier: Datenübermittlung) personenbezogener Daten und besonderen Arten von personenbezogenen Daten. Eine Übermittlung personenbezogener Daten käme gegebenenfalls unter den Voraussetzungen des § 23 Abs. 1 ThürDSG bzw. bei besonders geschützten Daten wie Gesundheitsdaten unter den Voraussetzungen in § 4 Abs. 5 Nr. 1 bis 8 ThürDSG in Betracht.

Aufgrund der Kurzfristigkeit des anstehenden Besuchs des CPT in Thüringer Justizvollzugsanstalten kam im vorliegenden Fall die Erteilung der Einwilligung der betroffenen Gefangenen (§ 4 Abs. 2,3, 5 Nr. 2 ThürDSG) für die Einsichtnahme in ihre Gefangenakte durch das CPT als eine datenschutzkonforme Lösung in Betracht. Die Einwilligung hat den Vorgaben des § 4 Abs. 3 ThürDSG zu entsprechen. Danach ist der Betroffene auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen (informierte Einwilligung). Der Betroffene ist auch darauf hinzuweisen, dass er seine Einwilligung jederzeit widerrufen kann. Die Einwilligung bedarf grundsätzlich der Schriftform. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die Einwilligung ist nur dann wirksam, wenn der Betroffene die Bedeutung und die Tragweite seiner Entscheidung zu überblicken vermag. Für besonders geschützte Daten (z. B. Gesundheitsdaten) gilt, dass die Einwilligung sich ausdrücklich auf diese Daten beziehen muss (§ 4 Abs. 5 Nr. 2 ThürDSG). Das TMMJV folgte der Einwilligungslösung, sieht aber – wie der TLfDI – die Schaffung einer eigenständigen Rechtsgrundlage für die Akteneinsicht durch Mitglieder des CPT als sachdienlich an.

Aus Gründen der Rechtssicherheit sieht der TLfDI die Schaffung einer eigenständigen gesetzlichen Grundlage für die Gewährung der Akteneinsicht für die Mitglieder des CPT als sachdienlich an, soweit diese zur Erfüllung der in Art. 8 der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe genannten Verpflichtung erforderlich ist. Der TLfDI wird die Einfügung einer solchen Grundlage in das Thüringer Justizvollzugsgesetzbuch im Auge behalten.

10.10 Neufassung des Thüringer Maßregelvollzugsgesetzes

Seit Anfang 2002 war der Maßregelvollzug in Thüringen infolge Beleihung auf private Träger übertragen. Eine Neuregelung wurde notwendig, weil das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung BVerfGE 130,76 Vorgaben für eine Privatisierung des Maßregelvollzugs aufgestellt hatte. Außerdem hatte das BVerfG in seinen Entscheidungen aus dem Jahr 2011 und 2013 (BVerfGE 128, 282; 129 269) festgelegt, dass die medizinische Zwangsbehandlung eines im Maßregelvollzug untergebrachten Patienten besonderer materiell-rechtlicher und verfahrensrechtlicher Voraussetzungen bedarf. Im Gesetz mussten daher vor allem die Regelungen zur Beleihung von psychiatrischen Kliniken in privater Hand angepasst werden, damit diese die hoheitliche Aufgabe des Maßregelvollzugs und zur medizinischen Zwangsbehandlung wahrnehmen können.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gab zu dem vom damaligen Thüringer Ministerium für Soziales, Familien und Gesundheit (TMSFG) übersandten Gesetzentwurf eine Stellungnahme ab und machte zahlreiche Änderungsvorschläge, von denen hier nur die wichtigsten dargestellt werden:
Nach der damals vorgesehenen Regelung zum Besuchsrecht konnte ein Besuch davon abhängig gemacht werden, dass sich der Besucher durchsuchen lässt, wenn Anhaltspunkte dafür bestanden, dass die Sicherheit der Einrichtung gefährdet wird. Bei der Durchsuchung eines Besuchers werden dessen personenbezogene Daten erhoben. Die Durchsuchung stellt damit einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Besucher dar. Dabei können Informationen zutage treten, die der höchstpersönlichen Lebenssphäre des Besuchers zuzuordnen sind. Ein derartiger Eingriff kann daher

nur bei einer konkreten Gefahr für die Sicherheit der Einrichtung zulässig sein. Eine Durchsuchung sollte daher nur bei konkreten Anhaltspunkten für eine Gefährdung der Sicherheit möglich sein. Zwar hat der Besucher die Wahl, ob er sich der Durchsuchung unterzieht, von einer tatsächlichen Freiwilligkeit kann hier aber nicht gesprochen werden, da die durchzuführende Maßnahme Voraussetzung dafür ist, dass der Patient besucht werden kann. (siehe dazu Nr. 11.9.).

Weiterhin sollte der Besucher aus Gründen der Behandlung und der Sicherheit des Patienten überwacht werden können. Bei einem Besuch wird der Patient mit dem Besucher in aller Regel eine Unterhaltung mit privatem Inhalt führen. Sofern diese überwacht wird, werden personenbezogene Daten des Patienten und des Besuchers erhoben. Nach Auffassung des TLfDI ist der bloße Bezug auf Gründe der Behandlung oder der Sicherheit des Patienten oder der Einrichtung aufgrund der Intensität des Eingriffes verfassungswidrig. Er forderte, im Gesetzentwurf klarzustellen, dass die Überwachung aus Gründen der Behandlung oder der Sicherheit des Patienten und der Einrichtung zwingend erforderlich ist bzw. unerlässlich sein muss.

Es sollte möglich sein, den Schriftwechsel eines Patienten sowie den Paketverkehr zu überwachen und Schreiben und Pakete anzuhalten, soweit es zur Verhinderung von Nachteilen für den Patienten, zur Sicherung des Zwecks zur Unterbringung, für die Sicherheit der Einrichtung oder zur Verhinderung einer Gefährdung bedeutender Rechtsgüter Dritter erforderlich war. Auch die Überwachung und ggf. die Anhaltung des Schriftverkehrs ist ein sehr starker Grundrechtseingriff, der nur gerechtfertigt sein kann, wenn er aus den angeführten Gründen unerlässlich ist. Der TLfDI regte daher an, auch hier eine zwingende Erforderlichkeit als Voraussetzung aufzustellen.

Nach einer Regelung konnten zur Verhinderung des Suchtmittelmissbrauchs der Patienten Kontrollen durchgeführt werden. Nicht dargelegt war, welcher Art diese Kontrollen sein sollten und unter welchen konkreten Voraussetzungen sie durchgeführt werden dürfen. Für Regelungen, die eine Ermächtigung zu Grundrechtseingriffen enthalten, gilt das Gebot der Normenklarheit und -bestimmtheit. Diesem widersprach die sehr allgemein gehaltene Formulierung.

Vollständig abgelehnt wurde eine Bestimmung, in der festgelegt wurde, was personenbezogene Daten im Sinne des Gesetzes sind. Dieser dort definierte Begriff widersprach demjenigen, der in den Datenschutzgesetzen definiert ist (vgl. § 3 Abs. 1 Bundesdaten-

schutzgesetz, § 3 Abs. 1 Thüringer Datenschutzgesetz, § 67 Abs. 1 Satz 1 Sozialgesetzbuch Zehntes Buch).
Da beabsichtigt war, besondere Arten von personenbezogenen Daten einem besonderen Schutz zu unterwerfen, sollten diese nach Auffassung des TLfDI als besondere Arten von personenbezogenen Daten im Gesetz näher definiert werden.
Da die Akten über Patienten nach dem Entwurf auch elektronisch geführt werden konnten, wies der TLfDI darauf hin, dass die elektronische Aktenhaltung zu höheren Risiken für den Datenschutz führt. Im Gegensatz zu den klassischen Papierakten können Daten in elektronischen Akten leichter ausgewertet, mit anderen Daten zusammengeführt oder verändert werden. Deshalb bedarf es bei der Einführung von elektronischen Akten deutlich höherer Anforderungen an die nach § 9 ThürDSG zu treffenden technischen und organisatorischen Maßnahmen zum Datenschutz. Zumindest hinsichtlich der Speicherung und der Übermittlung von personenbezogenen Daten sollten daher in das Gesetz auch technische Anforderungen aufgenommen werden. Die Videoüberwachung und Aufzeichnung von Außenanlagen, Gebäuden, der unmittelbaren Anstaltsumgebung sowie allgemein zugänglichen oder gemeinschaftlich genutzten Räumen und der Kriseninterventionsräume mittels optisch-elektronischer Einrichtungen war als zulässig vorgesehen, soweit dies zur Aufrechterhaltung und Gewährleistung der Sicherheit und Ordnung erforderlich ist. Auch bei dieser Maßnahme handelt es sich um einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung sowohl der Patienten als auch der Besucher und der in der Einrichtung beschäftigten Personen. Nach der Rechtsprechung des Bundesverfassungsgerichts muss ein derartiger Eingriff nicht nur zur Erreichung des Zwecks geeignet und erforderlich sein, er muss auch angemessen sein (Grundsatz der Verhältnismäßigkeit im engeren Sinne). Daher muss immer auch eine Abwägung mit den Grundrechten der potentiell Betroffenen stattfinden. Daher sollte die Vorschrift dahingehend ergänzt werden, dass eine Zulässigkeit nur gegeben ist, wenn schutzwürdige Belange der Betroffenen nicht überwiegen.
Die angeregten Änderungen wurden größtenteils übernommen. Im parlamentarischen Verfahren wurde der TLfDI nochmals zur Stellungnahme aufgefordert. Er wies darauf hin, dass eine Kontrolle von Besuchern auch zur Verhinderung des Suchtmittelmissbrauchs zum einen unverhältnismäßig sein dürfte und zum anderen auch der Re-

gelung widerspricht, nach der bei konkreten Anhaltspunkten dafür, dass ein Besucher selbst berauscht ist oder Drogen oder Rauschmittel in die Vollzugseinrichtung hineinbringen will, der Besuch davon abhängig gemacht werden kann, dass der Besucher sich geeigneten Maßnahmen zur Entkräftung des Verdachts unterwirft.
Da die Anregung des TLfDI nicht übernommen wurde, stellte der TLfDI nochmals die Forderung, dass bei Kontrollen zur Verhinderung des Suchtmittelmissbrauchs darzulegen ist, welcher Art diese Kontrollen sind und unter welchen konkreten Umständen sie durchgeführt werden dürfen. Diese Forderung wurde im parlamentarischen Verfahren leider nicht aufgegriffen.

Auch wenn das neugefasste Thüringer Maßregelvollzugsgesetz zahlreiche Verbesserungen für die Patienten enthielt, gab es bei einigen Regelungen aus Sicht des TLfDI noch Nachbesserungsbedarf aus datenschutzrechtlicher Sicht. Erfreulicherweise wurden die meisten Änderungsvorschläge in das neue Gesetz aufgenommen.

10.11 Den Wächtern auf der Spur

Die Justizvollzugsanstalt (JVA) Hohenleuben übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum eine geänderte Dienstvereinbarung zwischen dem Anstaltsleiter der JVA Hohenleuben und dem örtlichen Personalrat, verbunden mit der Bitte um eine datenschutzrechtliche Bewertung. Die Änderungen in der Dienstvereinbarung seien notwendig gewesen, da die Personennotrufanlage durch eine neue Anlage ersetzt worden sei. Der Zweck der Anlage bestünde darin, in besonderen Gefährdungslagen (z. B. Geiselnahme, Brand, Bombendrohung) Alarm auszulösen. Zudem sei es mit dieser Anlage möglich, den Ort des Alarms und damit die Position des jeweiligen Bediensteten feststellen zu können. Mithilfe der Daten könne darüber hinaus auch festgestellt werden, welche Wege die Bediensteten während der Arbeit gegangen sind. Aufgrund einiger Vorkommnisse in der JVA müsse die Bestreifung der Bediensteten kontrolliert werden. Mit der geänderten Dienstvereinbarung war beabsichtigt, die durchzuführenden Überprüfungen zu reduzieren, ohne jedoch ganz darauf zu verzichten. Vorgesehen hatte die JVA jährliche Kontrollen, bei denen jeweils im Folgejahr insgesamt 30 Auszüge ausgewählt und ausgewertet würden. Der TLfDI kriti-

sierte, dass sich in der Dienstvereinbarung kein Hinweis darauf befand, dass eine vollständige Verhaltens- und Leistungskontrolle der Bediensteten grundsätzlich ausgeschlossen ist. Auch unter Berücksichtigung der besonderen Voraussetzungen im Strafvollzug im Hinblick auf das Sicherheitsbedürfnis, war nach der Ansicht des TLfDI die Durchführung einer vollständigen und auf einzelne Personen zu beziehende Leistungs- und Verhaltenskontrolle nicht zu rechtfertigen. Daher empfahl der TLfDI die Aufnahme einer ergänzenden Formulierung, dass eine vollständige Verhaltens- und Leistungskontrolle einzelner Bediensteter grundsätzlich nicht zulässig ist. Die vom TLfDI vorgeschlagene Formulierung nahmen die Parteien der Dienstvereinbarung in diese auf.

Der Arbeitgeber ist zwar berechtigt, Kontrollen bzgl. der Arbeitsweise seiner Mitarbeiter bzw. Bediensteten durchzuführen. Eine vollständige verdachtsunabhängige Verhaltens- und Leistungskontrolle der Bediensteten ist aber grundsätzlich ausgeschlossen und damit unzulässig.

10.12 Auch für eine unklare Übergangsregelung läuft einmal die Zeit ab – zur Veröffentlichung von beeidigten Dolmetschern im Internet

Das damalige Thüringer Justizministerium (TJM) gab dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im November 2014 die Gelegenheit zur Stellungnahme im Anhörungsverfahren zur ersten Änderung der Thüringer Verordnung zur Regelung der allgemeinen Beeidigung von Dolmetschern und der Ermächtigung von Übersetzern (DolmV TH).
Obgleich der Änderungsentwurf lediglich das Datum des Außerkrafttretens aufhob, nutzte der TLfDI die „Gunst der Stunde“ zur inhaltlichen Stellungnahme zur DolmV TH. Denn diese besaß in § 2 Abs. 2 DolmV TH folgenden Wortlaut:
„(2) Abweichend von Absatz 1 Satz 3 bedarf es für die Veröffentlichung der Daten der bei Inkrafttreten dieser Verordnung bereits allgemein beeidigten Dolmetscher und ermächtigten Übersetzer im Internet keiner Einwilligung. Die Betroffenen werden spätestens sechs Wochen vor der Einstellung ihrer Daten ins Internet schriftlich informiert und können einer vollständigen oder teilweisen Veröffentlichung ihrer Angaben im Internet innerhalb von vier Wochen wider-

sprechen. Der Widerspruch ist schriftlich an den nach § 17 Abs. 1 Thüringer Gesetz zur Ausführung des Gerichtsverfassungsgesetzes (ThürAGGVG) zuständigen Präsidenten des Landgerichts zu richten. Auch nach der Veröffentlichung der Daten im Internet ist ein Widerspruch jederzeit möglich; Satz 3 gilt entsprechend."

Für den TLfDI war in erster Linie nicht nachvollziehbar, weshalb dieser Absatz überhaupt noch erforderlich sein sollte. Denn eigentlich war er doch bei Inkrafttreten der Verordnung im Jahr 2009 ausdrücklich als Übergangsvorschrift eingefügt worden. Der TLfDI vertrat deshalb die Ansicht gegenüber dem TJM, dass es dieser Übergangsvorschrift nach fünf Jahren nicht mehr bedürfe.

Weiterhin ergibt sich daraus im Umkehrschluss, dass nach Ablauf der Übergangszeit und Einrichtung einer länderübergreifenden Dolmetscher- und Übersetzerdatenbank (http://www.justiz-dolmetscher.de/) für alle beeidigten Dolmetscher und ermächtigten Übersetzer eine Einwilligung erforderlich ist, um ihre personenbezogenen Daten im Internet zu veröffentlichen. Denn zu beachten ist, dass die Veröffentlichung eines Verzeichnisses über beeidigte Dolmetscher und ermächtigte Übersetzer nach § 22 ThürAGGVG im Internet stets auch eine Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes darstellt, deren Zulässigkeit nach § 23 Thüringer Datenschutzgesetz (ThürDSG) zu beurteilen ist. Demzufolge verlangt § 23 Abs. 2 Nr. 1 ThürDSG für eine Übermittlung personenbezogener Daten in Drittstaaten, in denen kein angemessenes Datenschutzniveau im Sinne von § 23 Abs. 1 ThürDSG gewährleistet ist, die zweifelsfreie Einwilligung des Betroffenen.

In Anbetracht dessen regte der TLfDI an, dass die Einwilligung zur Veröffentlichung personenbezogener Daten im Internet im Rahmen der Veröffentlichung eines Verzeichnisses nach § 22 ThürAGGVG auch für bereits bei Inkrafttreten der Verordnung allgemein beeidigte Dolmetscher und ermächtigte Übersetzer einzuholen war.

Das TJM ist den Empfehlungen des TLfDI im Rahmen der Novellierung im Jahr 2014 nicht gefolgt. Zur Begründung verwies das TJM auf die Regelung des § 2 Abs. 3 der DolmV TH hin, wonach die Daten eines Dolmetschers oder Übersetzers ausschließlich in einem geschützten Bereich den Gerichten und Staatsanwaltschaften zur Verfügung gestellt würden, wenn diese in eine Veröffentlichung im

netzöffentlichen Verzeichnis nicht einwilligten oder ihr widersprächen.
Dieser Einwand überzeugte nach Auffassung des TLfDI aus zwei Gründen nicht: Zum einen betraf die Regelung des § 2 Abs. 3 DolmV TH nur das netzöffentliche Verzeichnis und nicht das Internet, sodass eine Einwilligung für die Veröffentlichung der personenbezogenen Daten im Internet nach wie vor erforderlich war. Zum anderen war auch kein sachlicher Grund für den TLfDI erkennbar, warum bei allen Dolmetschern und Übersetzern, die bei Inkrafttreten dieser Verordnung bereits vereidigt waren, eine Einwilligung zur Veröffentlichung ihrer personenbezogenen Daten im Internet entbehrlich sei. Darauf hingewiesen, stellte das TJM eine spätere Prüfung des datenschutzrechtlichen Problems in Aussicht. Wir bleiben dran.

Die Veröffentlichung von personenbezogenen Daten im Internet wird leider noch viel zu oft von öffentlichen Stellen unterschätzt: Denn damit gelangen diese Daten zugleich in Länder, in denen überhaupt kein oder nur ein spärliches Datenschutzniveau vorhanden ist. In diesen Drittstaaten – also solchen Ländern, in denen kein europäisches Datenschutzniveau gewährleistet ist – ist das Risiko einer rechtswidrigen Datenverarbeitung nicht gerade gering. Zu Recht verlangt daher § 23 Abs. 2 Nr. 1 ThürDSG, dass eine Datenübermittlung in einen solchen Drittstaat die zweifelsfreie Einwilligung des Betroffenen voraussetzt.

Family doctor woman. – © Kurhan / Fotolia.com

11 Arbeit, Gesundheits- und Sozialdatenschutz, Frauen und Familien

11.1 Logo arbeitsuchend? Jobcenter verwenden kein spezielles Logo

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine Information über zahlreiche bei ihr eingehende Beschwerden wegen der Verwendung von Logos, also von grafischen Zeichen, Buchstaben, Bildelementen usw. durch Jobcenter auf Briefumschlägen. Der TLfDI stimmte mit der Auffassung der BfDI überein, wonach es keine Erforderlichkeit gibt, Briefumschläge aus den Jobcentern mit einem

solchen Logo zu versehen, sodass hierdurch eventuell ein möglicher Leistungsbezug Dritten schon bei flüchtiger Betrachtung offenbart werden könnte. Der Gebrauch von solchen zusätzlichen Merkmalen in Form von Stempeln, Aufdrucken, Aktenzeichen usw. auf den Briefumschlägen steht dem Anspruch von Betroffenen auf Wahrung des Sozialgeheimnisses durch das Jobcenter gemäß § 35 Sozialgesetzbuch Erstes Buch entgegen. Die Stellen sind darüber hinaus auch nach § 78 a Sozialgesetzbuch Zehntes Buch gesetzlich verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, die den Anspruch auf Vertraulichkeit gewährleisten. Allerdings ist aus datenschutzrechtlicher Sicht die Nennung der Absenderadresse des Jobcenters erforderlich, um z. B. ansonsten unzustellbare Post an den Absender zurückzusenden. Dies geschieht am besten durch die Angabe lediglich des Postfachs. Auch die im Sichtfenster der Briefumschläge verwendeten Aktenzeichen oder Kundennummern lassen keine Rückschlüsse auf persönliche Daten der Betroffenen zu, da Dritte im Regelfall hiermit keine Verbindung zu einem Jobcenter herstellen können. Da der TLfDI bei den so genannten Optionskommunen in Thüringen, also bei Thüringer Kommunen, die die alleinige Trägerschaft der Leistungen nach dem Sozialgesetzbuch Zweites Buch besitzen, die datenschutzrechtliche Kontrollzuständigkeit innehat, sind diese Optionskommunen vom TLfDI angeschrieben, über die oben genannte Rechtsauffassung informiert und um Auskunft hinsichtlich des eigenen Gebrauchs von Logos aufgefordert worden. Im Ergebnis wurde dem TLfDI von den kommunalen Jobcentern mitgeteilt, dass dort jeglicher Schriftwechsel ohne Hinweise auf einen bestimmten Fachbereich oder Fachdienst das Jobcenter verlässt und daher auf den Briefumschlägen nicht erkennbar ist. Für den TLfDI war daher die Angelegenheit als erledigt anzusehen.

Sozialleistungsträger müssen im Briefverkehr mit dem Bürger auf die Gestaltung ihrer Briefumschläge mit Logos verzichten. Die Briefumschläge sind so zu gestalten, dass Dritte nicht ohne besonderen Aufwand einen Sozialleistungsträger als Absender erkennen können. Für erforderliche Rücksendungen, etwa wenn ein Brief nicht zugestellt werden kann, reicht die Angabe der Postfachadresse.

11.2 Originalunterlagen für das Jobcenter?

Aufgeregt meldete sich eine Thüringerin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), das Jobcenter gebe sich mit Kopien ihrer Unterlagen, insbesondere ihrer teilweise geschwärzten Kontoauszugskopien nicht zufrieden. Sie sei zwar auf die Leistungen angewiesen, lege aber trotzdem Wert auf den Datenschutz.

Der TLfDI stellte fest, dass das betroffene Jobcenter – da es sich nicht um eine Optionskommune handelte – nicht seiner, sondern der Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) unterlag. Dorthin verwies er die Beschwerdeführerin. In der Sache ist der Beschwerdeführerin Recht zu geben. Auch der TLfDI vertritt die Auffassung, dass im Rahmen des Antrags auf Arbeitslosengeld (ALG) II-Leistungen Unterlagen grundsätzlich nur zur Ansicht vorzulegen sind, sodass sich der Sachbearbeiter Notizen dazu machen kann. Im Einzelfall können auch Kopien verlangt werden, wobei Schwärzungen von Angaben, die für die Aufgabenerfüllung nicht erforderlich sind, zulässig sind. Zu weiteren Einzelheiten sind in diesem Zusammenhang die „Hinweise zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen“ hilfreich, die gemeinsam von verschiedenen Datenschutzbeauftragten der Länder veröffentlicht wurden und denen sich der TLfDI ebenfalls angeschlossen hat.

Sie können diese Hinweise im Internet unter https://www.datenschutzzentrum.de/artikel/824-Hinweise-zur-datenschutzgerechten-Ausgestaltung-der-Anforderung-von-Kontoauszuegen-bei-der-Beantragung-von-Sozialleistungen.html#extended aufrufen.

Im Rahmen des Antrags auf ALG II-Leistungen sind Unterlagen grundsätzlich nur zur Ansicht vorzulegen, sodass sich der Sachbearbeiter Notizen dazu machen kann. Im Einzelfall können auch Kopien verlangt werden, wobei Schwärzungen von Angaben, die für die Aufgabenerfüllung nicht erforderlich sind, zulässig sind.

11.3 Datensucht im Jobcenter

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von einem Betroffenen der Profilingbogen, also die Darstellung des beruflichen sowie des Persönlichkeits- und des Qualifikationsprofils, eines Jobcenters einer Optionskommune in Thüringen mit der Frage zugeleitet, ob er denn tatsächlich die Fragen beantworten müsse.

Der Beschwerdeführer war zum Zweck der Vermittlung in Arbeit oder Ausbildung bzw. der Vorbereitung von aktiven Arbeitsförderungsleistungen eingeladen worden. Zu dem Termin sollte er verschiedene Unterlagen und den besagten ausgefüllten Profilingbogen mitbringen, ansonsten drohten ihm verschiedene Sanktionen. Im Profilingbogen störten ihn insbesondere die Fragen, ob ein Entzug des Führerscheins vorliege und wenn ja, in welchem Zusammenhang (Alkoholmissbrauch oder Strafverfahren), ob er Suchtprobleme habe, Schulden, Vorstrafen oder ob er gar in Insolvenz gefallen war, oder ob er ehrenamtliche Tätigkeiten übernommen hatte und wenn ja, welche. Darüber hinaus enthielt aber der Profilingbogen auch noch andere Fragen, deren Zielrichtung zur Aufgabenerfüllung sich nicht auf den ersten Blick erschloss. Hierzu zählten insbesondere, ob der Betroffene selbstständig war und wieviel er verdiente, ob und welche gesundheitliche Einschränkungen vorlagen, ob ein amtsärztliches Gutachten erstellt worden war, welche Hobbies in der Freizeit ausgeübt wurden sowie zur finanziellen Situation.

Der TLfDI wandte sich an das Jobcenter und wies darauf hin, dass die Erhebung von Sozialdaten einer konkreten Rechtsgrundlage bedürfe, die weder aus dem Anschreiben an die Kunden noch aus dem Fragebogen selbst zu entnehmen seien. Im Übrigen dürften nach Auffassung des TLfDI nur dann Hinweise zu Leistungseinschränkungen aufgrund medizinischer Befunde oder festgestellter funktionsbedingter Behinderungen eintragen werden, wenn sie eine Eingliederung in den Zielberuf oder in bestimmte Ausbildungen erheblich erschweren. Diese Informationen kann der Leistungsberechtigte freiwillig geben; eine Erklärungspflicht besteht hier nicht. Die Feststellung der Leistungsfähigkeit obliegt vielmehr dem ärztlichen Dienst des Trägers der Grundsicherung. Hierauf müsse der Betroffene hingewiesen werden.

Das Jobcenter teilte mit, der Profilingbogen sei als Gesprächsleitfaden zu verstehen, aus dem das weitere erforderliche Handeln abge-

leitet werden könne. Die enthaltenen Angaben würden in der Regel mit den Leistungsberechtigten im persönlichen Gespräch geklärt. Manchmal würden die Bögen zur Vorbereitung für die Betroffenen auch vorab per Post zugesandt. Jedenfalls seien sensible Angaben zu Gesundheit, Finanzen, Süchten und Strafen freiwillig. Fehlende oder falsche Angaben hierzu hätten keine Konsequenzen, nur der Beratungsansatz könne dann nicht optimal sein. Alles diene dem Ziel einer schnellen Arbeitsmarktintegration.
Die Frage nach der Selbstständigkeit konnte vom Jobcenter damit begründet werden, dass dann ein bestimmter Fallmanager zuständig ist. Auch das daraus erzielte Einkommen war für die weitere Beratung begründbar.
Die Frage nach dem Führerschein habe den Hintergrund, dass dann von einer besseren Mobilität insbesondere im ländlich geprägten Bereich ausgegangen werden könne. Ein fehlender Führerschein sei ein Vermittlungshemmnis, das – sofern er nicht entzogen wurde – schnell beseitigt werden könnte. Aufgrund der Hinweise des TLfDI hat das Jobcenter dann aber doch die Frage nach dem Führerscheinentzug aus dem Fragebogen entfernt.
Suchtprobleme und auch größere finanzielle Probleme, so legte das Jobcenter dar, stünden in der Regel einer Arbeitsaufnahme entgegen und müssten vorrangig behandelt werden. Zielgerichtet beraten könne man aber nur, wenn das Problem benannt und bekannt sei. Gesundheitliche Einschränkungen hätten Einfluss auf die Zumutbarkeit der Aufnahme einer bestimmten Arbeit. Es würde Geld und Zeit ersparen, wenn der Betroffene hier freiwillig Angaben machte und entsprechende Belege vorlegte. Ansonsten müsste der Amtsarzt eingeschaltet werden.
Das Jobcenter hat den Profilingbogen entsprechend den Forderungen und Hinweisen des TLfDI überarbeitet. Insbesondere wurde deutlich gemacht, welche Angaben für welchen Zweck nur freiwillig zu machen und welche Angaben Pflicht sind. Der Fragebogen enthält daher immer noch eine Fülle von Fragen, die mit Sternchen gekennzeichnet und daher nur freiwillig zu machen sind. Genaue Angaben zu gesundheitlichen Einschränkungen sind nicht mehr vorgesehen; ebenso können keine „sonstigen Hinweise“ oder Angaben zur familiären Situation mehr gemacht werden. Ob jemand Suchtprobleme hat, kann er freiwillig angegeben, um ein Beratungsangebot zu erhalten. Das sollte reiflich abgewogen werden.

Auch wenn ein Fragebogen nur als Leitfaden für ein optimales Beratungsgespräch im Jobcenter dienen soll, dürfen die Fragen nicht über das erforderliche Maß hinausgehen. Pflicht zur Antwort besteht nur, wenn eine Rechtsgrundlage dies verlangt. Können Angaben freiwillig zugunsten des Betroffenen gemacht werden, sind sie deutlich als freiwillig zu kennzeichnen.

11.4 Datenabgleich durch Jobcenter

Ein Betroffener beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein kommunales Jobcenter einer kreisfreien Stadt. Dieses hatte ihn nämlich zur Mitwirkung nach § 60 Abs. 1 Sozialgesetzbuch (SGB) Erstes Buch (I) aufgefordert, seinen Arbeitslosengeld I-Bezug von der Agentur für Arbeit mitzuteilen. Dies konnte er sich nicht erklären, weil er zwar einen Antrag auf Grundsicherung nach Sozialgesetzbuch (SGB) Zweites Buch (II) beim Jobcenter gestellt hatte, aber keine ALG I-Leistungen von der Agentur für Arbeit des Landkreises bezog. Da ihm bekannt war, dass das Jobcenter regelmäßig zu Beginn eines jeden Quartals einen automatisierten Datenabgleich gemäß § 52 SGB II zum Zweck der Überprüfung seitens der Bundesagentur für Arbeit durchführt, ob und in welcher Höhe jemand Leistungen der Agentur als Träger der Arbeitsförderung nach dem SGB erhält, schlussfolgerte der Beschwerdeführer, das Jobcenter habe Daten über ihn erhoben und gespeichert, die es weder erheben noch speichern durfte.
Das vom TLfDI zur Stellungnahme aufgeforderte Jobcenter teilte mit, es habe mit der Agentur für Arbeit weder Daten ausgetauscht noch abgeglichen. Bei der laufenden Bearbeitung sei aufgefallen, dass der Beschwerdeführer möglicherweise einen Anspruch auf Arbeitslosengeld I erworben haben könnte, weil er Bundesfreiwilligendienst geleistet und dabei Einkommen erzielt hatte. Daher sei der Beschwerdeführer mit einem Schreiben aufgefordert worden, seinen Leistungsbescheid über die Bewilligung des Arbeitslosengeldes I vorzulegen. Da er aber nun Leistungen nach SGB II erhielt, habe das Jobcenter pflichtgemäß mit einem weiteren Schreiben an die Agentur für Arbeit auch gleich einen Erstattungsanspruch eingereicht. Schließlich dürfe ein Betroffener nicht gleichzeitig beide Leistungen beziehen. Auf beide Schreiben habe das Jobcenter allerdings keine Antwort erhalten. Diese Darlegung war plausibel und das Vorgehen

wurde, gestützt auf die angegebenen Rechtsgrundlagen, als datenschutzrechtlich zulässig angesehen.
Der TLfDI stellte fest, dass das vom Jobcenter an den Betroffenen gerichtete Schreiben zumindest missverständlich war. Dem Leser wurde nicht deutlich, dass lediglich der Sachverhalt, nämlich ob der Betroffene die bezeichneten Leistungen erhält, überprüft werden sollte. Vielmehr wurde in dem Schreiben ohne konkrete Hinweise bereits davon ausgegangen, dass die Leistungen erbracht werden, die durch den geforderten Bescheid nachzuweisen sind.
Offenbar hatte man einfach ein Formularschreiben genutzt, dessen Inhalt und Intention nicht auf den Sachverhalt passte. Der TLfDI wies das Jobcenter darauf hin, dass, wenn auf ein Formularschreiben zurückgegriffen werden soll, vor seiner Verwendung jeweils zu prüfen ist, ob der Inhalt auf den konkreten Fall zutrifft. Sind Sachverhalte ungeklärt, bedarf es einer Erläuterung für die Betroffenen. Diese Maßnahmen sind einfachste Mittel, um in Zukunft derartige Beschwerden zu vermeiden. Der Vorgang ist noch nicht abgeschlossen.

Besteht die Möglichkeit, dass einem Betroffenen verschiedene Sozialleistungen zustehen, kann seitens der Sozialbehörde nicht unterstellt werden, der Betroffene beziehe diese auch. Werden Formularschreiben genutzt, muss überprüft werden, ob sie für den konkreten Zweck geeignet sind. Sind Sachverhalte ungeklärt, bedarf es der Erläuterung für den Betroffenen.

11.5 Immer wieder Kontoauszüge für das Jobcenter

Wer Leistungen nach dem Sozialgesetzbuch beantragt, muss vieles zum Zweck der Prüfung der Hilfebedürftigkeit offenlegen. Im Falle der Grundsicherung für Arbeitsuchende ist nach § 9 Abs. 1 Sozialgesetzbuch (SGB) Zweites Buch (II) hilfebedürftig, wer seinen Lebensunterhalt nicht oder nicht ausreichend aus dem zu berücksichtigenden Einkommen oder Vermögen sichern kann. Das Geld fließt in der Regel über das Girokonto. Will das Jobcenter aber die Kontoauszüge haben, gibt es oft Vorbehalte: Was ist mit dem Bankgeheimnis? Es geht doch niemanden etwas an, wie und bei wem ich mein Geld ausgebe oder wem ich was schuldig bin oder von wem ich Geld bekomme! Teilweise doch, denn um die Anspruchsvoraussetzungen der Grundsicherungsleistungen zu ermitteln und zu überprüfen, be-

darf es der Vorlage der Kontoauszüge und einer Kontenübersicht, falls mehrere Konten vorhanden sind. Nach der Rechtsprechung des Bundessozialgerichts (Urteil vom 19. September 2008 – Az. B 14 AS 54/07 R) dürfen Sozialbehörden von Antragstellern Kontoauszüge von bis zu drei zurückliegenden Monaten anfordern. In Ausnahmefällen können auch Kontoauszüge für länger zurückliegende Zeiträume erforderlich sein, wobei die Gründe hierfür zu dokumentieren sind. Die Antragsteller dürfen auf ihren Kontoauszügen den Überweisungszweck und den Empfänger schwärzen, sofern es sich um so genannte besondere Arten personenbezogener Daten handelt, vgl. § 4 Abs. 5 Thüringer Datenschutzgesetz. Es geht also um Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben. Im Klartext sind das üblicherweise Beträge an Gewerkschaften, politische Parteien, Religionsgemeinschaften, Arzt- und Medikamentenüberweisungen usw. Auf die Möglichkeit der Schwärzung solcher Daten muss das Sozialamt hinweisen.

Eine Antragstellerin für Sozialleistungen beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil das Jobcenter ihr nach ihrer Berechnung einen nicht unerheblichen Betrag schulde und trug vor, das Jobcenter habe von ihr ungeschwärzte Originale der Kontoauszüge und Versicherungspolicen verlangt und hiervon Kopien gefertigt. Erst auf nachdrückliche Aufforderung seien ihr die Originale im unverschlossenen Umschlag auf dem Postweg zurückgegeben worden, wodurch Missbrauch Tür und Tor offen gestanden habe. Einem zur Stützung der Beschwerde beigefügten Bescheid des Jobcenters war zu entnehmen, dass die beantragten Leistungen versagt worden waren, weil die Originalunterlagen zum festgesetzten Termin nicht vorgelegen hätten.

Der TLfDI konfrontierte das Jobcenter mit den Vorwürfen und bat um Stellungnahme. Nach Prüfung des Sachverhalts teilte das Jobcenter dem TLfDI mit, die Betroffene stelle ihre Anträge, Unterlagen und Nachweise regelmäßig per E-Mail, Telefax und per Post. Zwar reiche es dem Jobcenter grundsätzlich vollkommen aus, wenn Kontoauszüge in Kopie eingereicht würden und darauf die zulässigen Schwärzungen aufgebracht wurden. Die Beschwerdeführerin würde jedoch sowohl den Anfangs- als auch den Endkontostand schwärzen und eigenhändige Veränderungen vornehmen, etwa Buchungstexte

und Ähnliches durch eigene Texte ersetzen. Mit derartigen Grundlagen könne man keine gesetzlich vorgeschriebene Prüfung durchführen. Im Übrigen verfahre man genau, wie von der oben zitierten Rechtsprechung verlangt.
Nach der Darlegung des Jobcenters und ergänzend aus der Durchsicht der umfangreichen Unterlagen, die die Beschwerdeführerin dem TLfDI zugeleitet hatte, konnten keine Hinweise auf die Verletzung datenschutzrechtlicher Vorschriften festgestellt werden.
Eine Übersendung von Originalunterlagen der Beschwerdeführerin in unverschlossenem Umschlag schloss das Jobcenter aus und verwies auf die Praxis, dass ein Versand immer in verschlossenem Umschlag erfolge. Damit stand wieder einmal Einlassung gegen Einlassung. Mangels weiterer konkreter Anhaltspunkte konnte nicht festgestellt werden, dass im Fall der Beschwerdeführerin vom üblichen Postversand abgewichen worden war. Der TLfDI konnte daher der Beschwerdeführerin nicht behilflich sein, was er ihr auch mitteilte.

Zur Prüfung der Voraussetzungen für Sozialleistungen nach dem SGB II kann das Jobcenter die Vorlage von Kontoauszügen verlangen. Grundsätzlich reichen Kopien aus, denen nur die für die Prüfung der Einkommens- und Vermögensverhältnisse erforderlichen Angaben zu entnehmen und Angaben zu besonders zu schützenden personenbezogenen Daten geschwärzt sind. Bestehen berechtigte Zweifel seitens des Jobcenters, kann die Vorlage der ungeschwärzten Originale verlangt werden, die aber nicht einbehalten werden dürfen.

11.6 Vorsicht bei der Akteneinsicht

Eine Bürgerin hatte sich nach § 11 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Sie gab an, dass mehrere öffentliche Stellen in Thüringen mit den personenbezogenen Daten ihres Ehemannes nicht gesetzeskonform umgegangen seien. Dem lag folgender Sachverhalt zugrunde: Beide Eheleute waren in einem Pflegeheim in Thüringen beschäftigt. Dabei hatte die Frau ein befristetes Arbeitsverhältnis, ihr Ehemann hatte eine feste Anstellung. Der Frau waren bei ihrer Tätigkeit etliche Missstände in dem Heim aufgefallen, die sie der Heimaufsicht, dem Thüringer Landesverwaltungsamt, meldete. Dieses führte eine Überprüfung des Heimes durch, die zunächst keine Erkenntnisse zu Missständen

brachte. Dem Ehemann sei daraufhin mit Verweis auf das Prüfprotokoll der Arbeitsvertrag gekündigt worden, da er als Beschwerdeführer genannt wurde. Im Nachhinein wurden aber die gemachten Vorwürfe bei späteren Kontrollen der Heimaufsicht bestätigt. Als Kündigungsgrund sei angeführt worden, dass der Ehemann erhebliche unbegründete Vorwürfe gegenüber seinen Kollegen im Pflegeheim erhoben habe. Den Unterlagen des geführten Kündigungsschutzprozesses war als Ergebnis der Heimprüfung zu entnehmen, es sei festzustellen, dass die „Vorwürfe der Familie“ X (genannt wurde der Familienname der Beschwerdeführerin) im Rahmen der Kontrolle nicht bestätigt werden konnten. Die Rechtsanwälte des Pflegeheims hätten in den Diensträumen des Thüringer Landesverwaltungsamtes Akteneinsicht genommen. Die Angabe des Familiennamens der Beschwerdeführerin war bei der Gewährung der Akteneinsicht nicht geschwärzt worden.

Außerdem legte die Beschwerdeführerin dar, sie habe eine Dienstaufsichtsbeschwerde über den Bearbeiter im Thüringer Landesverwaltungsamt an das damalige Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) als vermeintliche Aufsichtsbehörde gerichtet. Das TMSFG habe die Aufsichtsbeschwerde ohne ihr Einverständnis an das damalige Thüringer Innenministerium weitergeleitet.

Da der Bericht über die Kontrolle des Pflegeheims dessen Anwälten im Rahmen der Akteneinsicht ungeschwärzt zur Kenntnis gegeben wurde, lag eine Übermittlung der Daten der Beschwerdeführer an Dritte vor. Diese ist nur zulässig, wenn eine gesetzliche Übermittlungsbefugnis gegeben ist oder der Betroffene eingewilligt hat, § 4 Abs. 1 ThürDSG. Nach § 29 Abs. 1 Thüringer Verwaltungsverfahrensgesetz hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gewähren, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Hier bestanden für den TLfDI erhebliche Zweifel, ob diese Voraussetzungen im vorliegenden Fall auch für den Namen der Beschwerdeführerin gegeben waren. Es war nicht ersichtlich, aus welchen Gründen es für die Einrichtung erforderlich gewesen sein sollte, den Namen des Beschwerdeführers in Erfahrung zu bringen. Hierüber informierte der TLfDI auch das Thüringer Ministerium für Inneres und Kommunales als oberste Aufsichtsbehörde. Dieses hat das Landesverwaltungsamt angewiesen, bei Akteneinsichten zukünftig neben der Erforderlichkeit der Kenntnis der Unterlagen zur Gel-

tendmachung oder Verteidigung rechtlicher Interessen auch die Möglichkeit einer zumindest teilweisen Schwärzung von in Akten befindlichen personenbezogenen Informationen vor der Einsichtnahme zu prüfen.
Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) teilte mit, dass die Dienstaufsichtsbeschwerde seinerzeit zuständigkeitshalber an das damalige Thüringer Innenministerium als dienstaufsichtsführende Stelle über die Beschäftigten des Thüringer Landesverwaltungsamts weitergeleitet wurde. Die Zuständigkeit einer Behörde ist in einem Verfahren von Amts wegen zu prüfen. Die Weiterleitung eines Antrags an die zuständige Behörde steht im Ermessen der befassten Behörde. Hier ist kein Grund ersichtlich, warum eine Weiterleitung der Dienstaufsichtsbeschwerde hätte unterbleiben müssen. Es war der erklärte Wille der Beschwerdeführer, das Verhalten des Bearbeiters im Landesverwaltungsamt durch die zuständige Aufsichtsbehörde prüfen zu lassen. Darin war daher kein datenschutzrechtlicher Verstoß zu sehen. Über das Ergebnis der Prüfung sowie die Rechtsauffassung des TLfDI wurde die Beschwerdeführerin informiert.

Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffende Akten zu gewähren, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Diese Prüfung darf nicht nur generell erfolgen, sondern in Bezug auf alle in der Akte enthaltenen personenbezogenen Daten Dritter. Im Zweifel ist Einsicht in eine Kopie zu gewähren, in der die personenbezogenen Daten geschwärzt sind.

11.7 E-Health-Gesetz des Bundes

„Health“ bedeutet „Gesundheit“. Verwirrend scheint, dass manchmal von eHealth und dann wieder von mHealth zu lesen ist. Wenn der Begriff mHealth benutzt wird, ist man im Bereich der „mobilen Gesundheit“, der Gesundheits-Apps, die Ihnen oder/und auch medizinischem Fachpersonal versprechen, durch die Anwendung auf Laptops, Smarthphones oder nun beispielsweise digitalen Uhren Ihre Gesundheit verbessern zu können (siehe Nummer 11.8).
Der Begriff eHealth bedeutet „elektronische Gesundheit“ und umfasst die aktive Nutzung der Gesundheitskarte (siehe dazu Nummer

15.8) und die Telematik im Gesundheitsbereich, also generell die Nutzung von Informationstechnik innerhalb des Gesundheitswesens.
Hinsichtlich eHealth liegt derzeit beim Bundestag ein Gesetzesentwurf „Gesetz für sichere digitale Kommunikation und Anwendung im Gesundheitsbereich“ vor (E-Health-Gesetz). So soll per Gesetz die medizinische Versorgung durch moderne Informations- und Kommunikationstechnologien verbessert werden. Ziel dabei ist es unter anderem, die Einführung der elektronischen Gesundheitskarte einschließlich ihrer nutzbringenden Anwendungen zu unterstützen und die Telematik und die Interoperabilität der informationstechnischen Systeme im Gesundheitswesen zu verbessern. Unter Interoperabilität versteht man, dass Geräte oder Anwendungen (Software) so gestaltet, also so standardisiert werden, dass sie mit anderen Geräten oder Systemen zusammenarbeiten können. Auch der Patienten-Nutzen würde sich dadurch erhöhen, da eine zielgenauere und schnellere Behandlung möglich wäre und auch gefährliche Wechselwirkungen, z. B. durch das Erfassen von verordneten Medikamenten, verringert werden könnte.
Aus datenschutzrechtlicher Sicht gibt es allerdings zurzeit noch Bedenken.
Deshalb erachtete die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder es im März 2015 für notwendig, in einer entsprechenden Entschließung Nachbesserungen zum Gesetzesentwurf zu fordern (siehe dazu Anlage 26). So mahnte sie insbesondere an, die Vertraulichkeit der Daten und Transparenz der Datenverarbeitung zu regeln. Da die Betroffenen selbst über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte entscheiden können, bedarf es eben der Transparenz, welche Daten durch wen verarbeitet werden können. Außerdem muss zu jeder Zeit die gebotene Vertraulichkeit der Daten gewährleistet sein. Auch im Hinblick darauf, dass insbesondere durch immer modernere Informationstechnik die Einschaltung externer Dienstleister durch Berufsgeheimnisträger nicht ausbleiben wird, bedarf es neben der technischen Sicherstellung der Vertraulichkeit weiterer Regelungen. Um nicht in die Gefahr eines Verstoßes gegen die Schweigepflicht (§ 203 StGB) zu kommen, gilt es, klare Rahmenbedingungen zu schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger überhaupt externe Dienstleister einschalten dürfen.

Bei der Verarbeitung personenbezogener Daten im Gesundheitswesen spielt die Vertraulichkeit der Daten und die Transparenz der Datenverarbeitung eine wichtige Rolle. Um nicht in die Gefahr eines Verstoßes gegen die ärztliche Schweigepflicht zu kommen, gilt es auch, klare Rahmenbedingungen zu schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen.

11.8 Mobile-Health-Dienste (mHealth) – der Datenmarkt boomt!

Gehören Sie auch zu den gesundheitsbewussten Menschen, die täglich Ihre Armbänder, Brustbänder oder eine entsprechende moderne Uhr bei sich tragen, damit diese Geräte Ihre Fitness überprüfen? Zählen Sie täglich elektronisch Ihre Schritte und Ihren Kalorienverbrauch per App (App = Applikationsoftware)? Schlafen Sie nachts mit einem eingeschalteten Smartphone neben sich, damit eine App Ihren Nachtschlaf überwacht?
Dieser neu kreierte Markt der Apps kann nützlich sein, er birgt aber auch datenschutzrechtliche Risiken. Zunächst gilt es, zwischen den verschiedenen Anwendungen hinsichtlich deren Zweck und Nutzen zu unterscheiden. So gibt es fachlich fundierte Apps, die rein informativ sind, also Informationen liefern, ohne Daten des Nutzers zu erfassen (z. B. Hinweise zur Ernährung, zur Gesundheitsvorsorge, zur Suchtberatung etc.). Es gibt aber auch Apps, die zum Beispiel im Pflegebereich genutzt werden können, bei denen Daten des Patienten gespeichert werden, um eine Erleichterung der Arbeit des Pflegepersonals und/oder des Arztes herbeizuführen. Und dann gibt es Apps, bei denen der Benutzer freiwillig seine personenbezogenen Daten eingibt und eine Datenauswertung anhand dieser Daten erfolgt. Die grundlegende Gefahr bei solchen mobilen Gesundheitsdiensten besteht darin, dass viele dieser Dienste einen gesundheitlichen Mehrwert versprechen, im Hintergrund aber eine Profilbildung des Benutzers erfolgen kann, auch durch Dritte, an die diese Daten unbemerkt übermittelt werden. Eine solche Profilbildung kann sich im Nachhinein zum Beispiel für eine gezielte Werbung lohnen. Nicht außer Acht zu lassen ist auch ein mögliches Interesse der Versicherungen an den Daten des Benutzers, um beispielsweise die Höhe von Kranken- und Lebensversicherungsbeiträgen zu bestimmen. Für einen gesunden Menschen dürfte die Datenauswertung noch kein Problem darstellen, schließlich profitiert er in den meisten Fällen zunächst

von einer gesunden Lebensweise. Anders sieht es aus, wenn sich zum Beispiel der Gesundheitszustand verschlechtert. In einem solchen Fall könnte sich der Betroffene zum „Risiko“ entwickeln, was sich gegebenenfalls auf die Beitragshöhe seiner Krankenversicherung auswirken könnte.

Auch Arbeitgeber könnten Interesse an mobilen Gesundheits-Apps finden. Unternehmen können schon jetzt ihren Mitarbeitern Apps anbieten, die messen, unter welchem Stresspegel die Mitarbeiter bestimmte Handlungen vornehmen (z. B. beim Telefonieren). Auch der Schlafrhythmus kann überwacht werden. Über einen längeren Zeitraum wird es so möglich, ein sehr genaues Bild von den Belastungen der Mitarbeiter zu erhalten (z. B. zu welcher Tageszeit der Stress besonders hoch ist). Das Unternehmen kann dadurch im besten Falle den Stress der Mitarbeiter früher erkennen und „Vermeidungsstrategien“ entwickeln. Für welchen Zweck das Unternehmen die Daten in der Praxis vielleicht noch verwenden könnte, bleibt ungewiss. „Natürlich“ entscheidet der Mitarbeiter „freiwillig“, ob er sich diese App auf seinem Smartphone installiert. Nein – im Ernst: Im Verhältnis zwischen Arbeitgeber und Arbeitnehmer sind derartige „Einwilligungen“ grundsätzlich unzulässig.

In dem „Aktionsplan für elektronische Gesundheitsdienste 2012–2020 – innovative Gesundheitsfürsorge im 21. Jahrhundert“ (Mitteilung der europäischen Kommission) wurde ein Grünbuch (= Diskussionspapier der Kommission) angekündigt, mit dem der Ausbau und das weitere Vorgehen in Bezug auf Mobile-Health-Dienste („mHealth“) eingeleitet werden sollte. Im April 2014 präsentierte die Europäische Kommission dann das Grünbuch über Mobile-Health-Dienste („mHealth“). Das Grünbuch definiert Mobile-Health als medizinische Verfahren und Praktiken der Gesundheitsfürsorge, die durch Mobilgeräte unterstützt werden. Zu den Mobilgeräten zählen nach dieser Definition unter anderem Mobiltelefone, Patientenüberwachungsgeräte, persönliche digitale Assistenten und andere drahtlos angebundene Geräte.

Es ist unbestritten, dass „mHealth“ ein großes Potenzial zur Verbesserung der medizinischen Prävention und Versorgung haben kann. Dennoch muss die datenschutzkonforme Verarbeitung der mitunter auch sehr sensiblen Gesundheitsdaten gewährleistet werden.

Bekannt ist, dass solche Apps eine nicht unerhebliche Menge personenbezogener Daten der Benutzer sammeln. Eine Verarbeitung dieser Daten muss dabei nicht in Deutschland stattfinden, sondern kann

möglicherweise auch in einem Drittstaat erfolgen. Ob in diesem Drittstaat ein angemessenes Datenschutzniveau herrscht, ist ungewiss.
Datenschutzrechtliche Bedenken sieht der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch im Hinblick auf eine mögliche Übermittlung der teilweise sensiblen personenbezogenen Daten – ob nun gewollt oder ungewollt – zum Beispiel an den Arbeitgeber, an die Versicherung oder an einen sonstigen Dritten.
Auch an die technischen und organisatorischen Maßnahmen für den Einsatz solcher Apps sind hohe Anforderungen zu stellen. Es muss aus datenschutzrechtlicher Sicht sichergestellt werden, dass die mitunter sehr sensiblen Daten nicht in die Hände unberechtigter Dritter gelangen und sie für Zwecke, zu denen der Betroffene nicht zugestimmt hat, verwendet werden. Dem Zweckbindungsgrundsatz ist in diesem Sinne eine hohe Bedeutung zuzumessen.
Schließlich gilt es zu bedenken, dass in Zeiten von „Big Data“ die Möglichkeit besteht, Datensätze durch die Verwendung von Algorithmen in Verbindung zu setzen und zu analysieren. Die aufbereiteten analysierten Informationen können unter Umständen für einen Dritten sehr wertvoll sein, nicht stets aber auch für den Betroffenen.
Im Berichtszeitraum beschäftigte sich auch der Europaausschuss des Thüringer Landtages mit dem Thema „Grünbuch der Kommission über Mobile-Health-Dienste („mHealth“)“ und lud hierzu den TLfDI ein, um dieses Thema zu erörtern. Dabei wies der TLfDI unter anderem darauf hin, dass der Nutzer grundsätzlich das Recht habe, die Nutzung dieser Dienste abzulehnen bzw. einen Anspruch auf Löschung seiner erfassten Daten habe, wenn er die Dienste nutze.
Weiterhin wies der TLfDI darauf hin, dass die Nutzung von Cloud-Computing Services (= Speichern von Daten jenseits des eigenen Personalcomputers, z. B. in entfernten Rechenzentren) zur Verarbeitung von Gesundheitsdaten datenschutzrechtlich problematisch sei und eine cloud-basierte Verarbeitung nur dann erfolgen könne, wenn sie über die Cloud sicher sei und die Zugriffsrechte eindeutig festgelegt seien und eine Datenübertragung verschlüsselt erfolge. Vor Akzeptanz der Allgemeinen Geschäftsbedingungen, in der eine datenschutzrechtliche Einwilligung erblickt werden kann, ist also Vorsicht mehr als geboten!
Eine Nachfrage des TLfDI beim Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) ergab, dass

die in Thüringen ansässigen Krankenkassen derzeit noch nicht an der Nutzung mobiler Gesundheitsdienste arbeiten bzw. diese planen.
Mit Inkrafttreten der Datenschutzgrundverordnung im Jahr 2016 wird dieses Thema datenschutzrechtlich neu zu bewerten sein. Der TLfDI wird deshalb weiterhin konstruktive Gespräche zu dem „Großprojekt“ Mobile-Health führen und alle Interessierten dazu beraten.

Apps im Gesundheitsbereich können sinnvoll sein, soweit sie zur Verbesserung der Gesundheit des Nutzers beitragen. Der Schutz personenbezogener Daten muss jedoch gewährleistet sein. So ist zum Beispiel dem Zweckbindungsgrundsatz der personenbezogenen Daten insoweit Rechnung zu tragen alsein unberechtigter Zugriff etwaiger Krankenkassen, Versicherungsunternehmern, Personalabteilungen und sonstigen Dritten auf die personenbezogenen Daten vermieden wird. Der Betroffene muss bei Akzeptanz der diesbezüglichen Allgemeinen Geschäftsbedingungen erhöhte Vorsicht walten lassen! Der TLfDI wird die Entwicklungen auf diesem „Markt der unbegrenzten Möglichkeiten“ weiter im Auge behalten.

11.9 Maßregelvollzug: Besuch nur mit Drogenscreening?

Von einer Abgeordneten im Thüringer Landtag erfolgte der Hinweis auf Probleme bei der Besucherkontrolle in Einrichtungen des Thüringer Maßregelvollzugs. Dort würden nämlich Besuche davon abhängig gemacht, dass Besucherinnen und Besucher Urin- und Speichelproben zur Untersuchung auf Drogenkonsum abgeben.
Das zuständige Ministerium (damals TMSFG – heute TMASFGG) antwortete selbst auf die Nachfrage des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bei der betroffenen Einrichtung. Es teilte im November 2014 mit, die angefragte Thematik der Besucherkontrollen im Maßregelvollzug sei mittlerweile durch das am 28. August 2014 in Kraft getretene Thüringer Maßregelvollzuggesetz (ThürMRVG) obsolet geworden. Nach § 17 Abs. 2 ThürMRVG könne nämlich ein Besuch, soweit konkrete Anhaltspunkte dafür bestehen, dass ein Besucher selbst berauscht ist oder Drogen oder Rauschmittel in die Vollzugseinrichtung hinein bringen will, davon abhängig gemacht werden, dass sich der Besucher „geeigneten Maßnahmen zur Entkräftung des Verdachts“ unterwirft. Dies stellte aus Sicht des TLfDI nicht die erforderliche,

hinreichend bestimmte Rechtsgrundlage für die Untersuchung von Urin oder Körperzellen und eine damit verbundene Verarbeitung entsprechender personenbezogener Daten der Besucher dar. Auf dieser Rechtsgrundlage kann nach Auffassung des TLfDI nicht gefordert werden, dass der bestehende Verdacht im Einzelfall durch die Abgabe von Urin-, Blut- oder Speichelproben ausgeräumt werden muss. Allein dadurch, dass der Besuch verweigert werden kann, wenn „konkrete Anhaltspunkte“ dafür bestehen, dass der Besucher selbst unter Einfluss von Rauschmitteln steht, sind weitergehende Prüfungen, etwa durch die Untersuchung von Körperzellen oder Flüssigkeiten, verbunden mit Eingriffen in das informationelle Selbstbestimmungsrecht nicht mit umfasst.

Daher wäre die Verarbeitung von Daten aus einer Untersuchung von Urin-, Blut- oder Speichelproben nur auf Einwilligungsbasis zulässig. An die Einwilligung im datenschutzrechtlichen Sinne sind nach § 4 Abs. 2 und 3 ThürDSG verschiedene Voraussetzungen geknüpft. Zum einen muss die Einwilligung auf einer freien Willensentscheidung beruhen. Zum anderen ist sie in der Regel schriftlich zu erteilen. Dabei sind Betroffene auf den konkreten Zweck und Umfang der Datenverarbeitung und auf Verlangen auf die Folgen der Verweigerung hinzuweisen. Sind Speicherungen der Ergebnisse von Tests auf Dogenkonsum beabsichtigt, ist dies deutlich zu machen. Ebenso ist über die Dauer der beabsichtigten Speicherung zu informieren. Da diese Vorgaben nicht eingehalten wurden, waren sowohl die Untersuchungen als auch die Speicherung der daraus erlangten Erkenntnisse ohne Rechtsgrundlage erfolgt. Im Übrigen wurde auch keine Erforderlichkeit für die Speicherung des Ergebnisses der durchgeführten Tests begründet.

Vor der Neuregelung in § 17 Abs. 2 ThürMRVG wurde von den Besuchern auf der Grundlage des § 19 Thüringer Gesetz zur Hilfe und Unterbringung psychisch kranker Menschen (ThürPsychKG) nach Darlegung des TMSFG / TMASGFF das Angebot unterbreitet, sich einem Alkohol- bzw. Drogentest zu unterziehen. Mit der Annahme dieses Angebots war aber auch damals keine wirksame Einwilligung im Sinne des § 4 ThürDSG erteilt worden. Somit war auch in der Vergangenheit die Datenverarbeitung ohne Rechtsgrundlage erfolgt.

Da also die mit der Durchführung von Drogenscreenings verbundene Datenverarbeitung sowohl nach dem alten Verfahren auf der Grundlage des § 19 PsychKG als auch nach dem neuen Verfahren auf der

Grundlage des § 17 Abs. 2 ThürMRVG rechtswidrig war, hat der TLfDI gefordert, dass die Daten gelöscht werden.
Das TMASGFF hat die Einstellung von Drogenscreenings auf der genannten, nicht ausreichenden Rechtsgrundlage und die Löschung der bisher erhobenen Daten zugesagt. Es wurde mitgeteilt, dass der Aktenbestand sukzessive nach so genannten Besucherlisten durchsucht wird, auf denen die Ergebnisse der Untersuchungen vermerkt sind, um diese zu vernichten.

Für die Verarbeitung personenbezogener Daten sind normenklare Rechtsgrundlagen erforderlich. Bestehen solche nicht, kann unter dem Gesichtspunkt der Erforderlichkeit eine Datenverarbeitung auf Einwilligungsbasis erfolgen. Die Einwilligungserklärungen müssen allerdings den Anforderungen des § 4 ThürDSG Rechnung tragen. Der Besuch im Maßregelvollzug kann unter diesen Voraussetzungen zwar davon abhängig gemacht werden, dass sich der Besucher freiwillig einem Drogenscreening unterwirft; für die Speicherung des Ergebnisses besteht jedoch nach wie vor keine Rechtsgrundlage.

11.10 Wenn der Arzt kommt – Erfassung von Einsatzdaten des kassenärztlichen Notdienstes

Die Kassenärztliche Vereinigung Thüringen hat die ambulante vertragsärztliche Versorgung in Thüringen sicherzustellen, allgemein bekannt als der Kassenärztliche Notfalldienst. Die Sicherstellung umfasst vor allem die ambulante Versorgung zu den sprechstundenfreien Zeiten (Notdienst). Die Versorgung der nicht-gehfähigen Patienten im ärztlichen Notdienst wird durch Fahrdienste sichergestellt, welche dann direkt zum Patienten fahren.
Die Fahrten und der getätigte medizinische Einsatz müssen durch den diensthabenden Arzt und dessen Assistenzpersonal dokumentiert werden. Um diese Protokollierung teilweise zu automatisieren und zumindest zu digitalisieren, setzt die Kassenärztliche Vereinigung Thüringen seit 2015 ein System ein, mit dem die durchgeführten Fahrten und die ärztlichen Einsätze zentral digital erfasst werden können. So werden bspw. auch personenbezogene Daten des Hilfesuchenden wie der Name, die Versicherungsnummer und durchgeführte Untersuchungen (ohne Diagnosen) erfasst. Diese Erfassung erfolgt entweder über Tablet oder PC mittels https oder optional über eine entsprechende mobile App (für Android).

Da diese Daten einem besonderen Schutz unterliegen, wandte sich die Kassenärztliche Vereinigung Thüringen zuvor an den TLfDI. So ist nun über ein Rollen- und Berechtigungskonzept geregelt, was z. B. ein „Administrator“, ein „Auswerter“ oder ein „Erfasser“ alles an Daten erfassen, sehen und verändern darf. Außerdem wurden die technischen Sicherheitsmaßnahmen der beteiligten Systemkomponenten bewertet.
Besonderes Augenmerk fiel der mobilen App zu, da bei dieser auf einem tragbaren Endgerät, wie z. B. einem Tablet oder Smartphone, die Daten für einen vorgegebenen Zeitrahmen gespeichert werden. Hier war insbesondere die Gefahr zu beachten, dass bei Verlust des Gerätes auch unberechtigte Dritte an persönliche Daten von Patienten gelangen könnten. Daher wurde mit den Entwicklern der App gemeinsam die Datensicherheit auf dem Gerät diskutiert. Neben der Notwendigkeit der Anmeldung bei Dateneingabe wurde noch eine zusätzliche Authentifizierungsstufe bei lesendem Zugriff auf die gespeicherten Daten hinzugefügt. Auch die verschlüsselte Übertragung sowie die verschlüsselte Datenspeicherung und die Datenlöschung bei der Nutzung der App waren ein Datenschutzthema. Zusätzlich dürfen nur dienstliche Tablets und Smartphones genutzt werden, um diese aus Sicherheitsgründen zentral administrieren zu können und nur dienstlich notwendige Apps für den Einsatz zuzulassen. Damit wird auch die Vermischung von dienstlichen und privaten Daten unterbunden.

Insbesondere bei dem Einsatz von Smartphones und Tablets, mit denen Patientendaten verarbeitet werden, ist darauf zu achten, dass ausschließlich dienstliche Geräte verwendet werden, um diese aus Sicherheitsgründen zentral administrieren und nur dienstlich notwendige Apps für den Einsatz zulassen zu können. Damit wird auch die Vermischung von dienstlichen und privaten Daten unterbunden. Zusätzlich sind die Daten nach dem Stand der Technik zu verschlüsseln.

11.11 Diagnose des Arztes auf dem Rezept: Geheimnisverrat gegenüber der Beihilfestelle

Die Beamten des Freistaats Thüringen werden im Krankheitsfall von der Beihilfestelle finanziell unterstützt. Hierfür müssen sie die ärztlichen Rechnungen bzw. Rezepte einreichen und einen Antrag auf

Erstattung stellen. Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag die Beschwerde eines Beihilfeberechtigten vor, der sich darüber beschwerte, dass die Beihilfestelle forderte, die Ärzte sollten in den Rezepten die ärztliche Diagnose angeben. Als Grund hierfür wurde genannt, dass anderenfalls die medizinische Notwendigkeit der Medikation nicht geprüft werden könne.
Die Angabe der Diagnose im Rezept stellt eine Übermittlung von personenbezogenen Daten an Dritte, beispielsweise den Apotheker, dar. Hierbei handelt es sich um Gesundheitsdaten, die nach dem Gesetz einem besonderen Schutz unterliegen, § 4 Abs. 5 Thüringer Datenschutzgesetz. Die Angabe ist datenschutzrechtlich unzulässig. § 2 Abs. 1 der Verordnung über die Verschreibung von Arzneimitteln legt fest, welche Angaben in einer Verschreibung zwingend enthalten sein müssen. Die Diagnose ist hier nicht genannt. Vielmehr ist davon auszugehen, dass der Arzt sich wegen Verletzung des Berufsgeheimnisses strafbar macht (§ 203 Strafgesetzbuch), wenn er die Diagnose auf dem Rezept vermerkt.
Nach § 7 Abs. 1 Satz 1 der Thüringer Beihilfeverordnung wird Beihilfe nur gewährt, wenn die Aufwendung medizinisch notwendig war. Es kann daher im Einzelfall erforderlich sein, die medizinische Notwendigkeit einer Verschreibung überprüfen zu müssen. Dies kann aber nicht regelmäßig erfolgen, sondern es ist davon auszugehen, dass bei einer ärztlichen Verschreibung grundsätzlich eine medizinische Notwendigkeit besteht. In Zweifelsfällen kann aber der Nachweis der medizinischen Notwendigkeit gefordert werden. Dies ist beispielsweise durch eine ärztliche Bescheinigung möglich. Die Beihilfestelle hat keinen Einfluss darauf, ob ein Arzt bei der Ausstellung eines Rezeptes die Angabe der Diagnose, die der ärztlichen Verordnung zugrunde liegt, mit auf dem Rezept vermerkt. Die Beihilfestelle hat aufgrund des Einschreitens des TLfDI den Erläuterungstext im Beihilfebescheid dahingehend geändert, dass nunmehr nicht der Vermerk der Diagnose auf dem Rezept, sondern die Vorlage von Unterlagen gefordert werden kann.

Es ist datenschutzrechtlich unzulässig, wenn Ärzte die Diagnose auf einem Rezept vermerken. Die medizinische Notwendigkeit einer Verschreibung kann gegenüber der Beihilfestelle durch Vorlage anderer geeigneter Unterlagen belegt werden.

11.12 Privatadressen von Ärzten: Herausgabe durch Krankenhaus?

Die Landesärztekammer Thüringen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie von einer Klinik die Privatadressen von Ärzten aus Datenschutzgründen nicht erhielt. Hintergrund war folgender:
Mitglied der Landesärztekammer Thüringen wird ein Arzt nach § 2 Abs. 1 Thüringer Heilberufegesetz (ThürHeilBG), sobald er in Thüringen eine ärztliche Tätigkeit aufnimmt, oder, wenn er keine ärztliche Tätigkeit ausübt, er seinen gewöhnlichen Aufenthalt hier hat. Dies gilt auch für Ärzte, welche als Honorarärzte an wechselnden Einsatzorten im ganzen Bundesgebiet tätig werden, oder für solche, die in einem anderen Bundesland ihre Haupttätigkeit ausüben und regelmäßig nebenberuflich in Thüringen arbeiten. In letzter Zeit häuften sich die Fälle von Ärzten, welche honorarärztlich kurzfristig (zwischen wenigen Tagen und mehreren Monaten), oft auch mehrmals in Kliniken oder anderen Einrichtungen in Thüringen ärztlich tätig werden und sich nicht bei der Kammer anmelden. Nach § 2 Abs. 2 ThürHeilBG sind die Ärzte verpflichtet, sich binnen eines Monats, bei vorübergehender Ausübung der Tätigkeit innerhalb von fünf Tagen nach Aufnahme der Tätigkeit, bei der Landesärztekammer anzumelden. Kammerangehörige, die dieser Verpflichtung nicht nachkommen, können nach § 11 ThürHeilBG mit einem Ordnungsgeld von bis zu 5.000 Euro belegt werden. Die Verhängung dieses Ordnungsgeldes ist dem Pflichtigen vorher schriftlich anzukündigen, was nur möglich ist, wenn seine Privatanschrift bekannt ist.
Nach § 19 Thüringer Datenschutzgesetz (ThürDSG) ist die Erhebung der notwendigen Daten durch die Landesärztekammer Thüringen zunächst bei dem Betroffenen zu veranlassen, Grundsatz der Datenerhebung beim Betroffenen. Möglich ist es auch, sich eines so genannten Adressmittlungsverfahrens zu bedienen, bei dem derjenige, der in Kenntnis der Adresse der Person ist, an die das Schreiben gerichtet werden soll, gebeten wird, das Schreiben an den Adressaten weiterzuleiten. Dieses Verfahren wurde bereits durchgeführt und führte nicht in allen Fällen zum Erfolg.
Nach § 19 Abs. 2 Satz 1 Nr. 2 bzw. 3 ThürDSG dürfen die Daten ohne die Mitwirkung des Betroffenen erhoben werden, wenn die zu erfüllende Aufgabe (hier die Registrierung und Berufsaufsicht) ihrer Art nach die Erhebung bei anderen Personen oder Stellen erforder-

lich macht oder die Erhebung bei dem Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. So lag der Fall hier. Die persönlichen Daten des Arztes werden benötigt, um den Arzt als Mitglied registrieren zu können und im Falle des Verstoßes gegen die Berufspflichten gegebenenfalls Sanktionen zu verhängen. Eine Zustellung der Ordnungsgeldanhörung oder sonstiger offizieller Schreiben (z. B. Beitragsbescheide) per Zustellungsurkunde an die betreffende Einrichtung hat dann keinen Erfolg, wenn der Arzt dort in aller Regel nicht mehr dienstlich tätig ist. Die Kammer hatte keine anderen Mittel, um die Privatadresse des Arztes in Erfahrung zu bringen. Insbesondere war eine Melderegisterauskunft nicht möglich, da außer dem Namen keine weiteren Daten bekannt sind. Die Privatadresse der Ärzte darf daher bei der Klinik erfragt werden, wenn die Versuche der Kammer, über die einzig bekannte ehemalige Dienstadresse des Arztes eine Zustellung zu erreichen, nicht zur Erfüllung der gesetzlichen Anmeldepflicht geführt haben.

Die für die Aufgabenerfüllung einer öffentlichen Stelle notwendigen personenbezogenen Daten müssen grundsätzlich beim Betroffenen erhoben werden. Etwas anderes gilt, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach die Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung bei dem Betroffenen einen unverhältnismäßigen Aufwand erfordert, § 19 Abs. 2 ThürDSG.

11.13 Rücksendung von Arztrechnungen und Rezepten an eine andere Beihilfeberechtigte

Eine Thüringer Beamtin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie die von ihr der Beihilfestelle zur Abrechnung eingereichten Arztrechnungen und Rezepte mit einem Fax-Aufdruck einer Thüringer Polizeidienststelle zurückerhielt. Sie bat um Prüfung, weshalb ihre sensiblen Patientendaten denn bei der Polizei gelandet waren, denn sie war weder im Polizeidienst noch konnte sie sich erklären, weshalb die Beihilfestelle die Polizei eingeschaltet haben sollte.
Auf Nachfrage des TLfDI erklärte die Beihilfestelle, ihre Mitarbeiter seien sich sehr darüber bewusst, dass sämtliche Angelegenheiten, die der Beihilfestelle im Zusammenhang mit der Bearbeitung von Beihilfeanträgen bekannt werden, einem besonderen Schutz unterlägen.

Auch im vorliegenden Fall habe es keine Einbeziehung einer Polizeidienststelle gegeben. Aufgrund der vielen Anträge, die jährlich zu bearbeiten seien, sei es jedoch leider dazu gekommen, dass die von der Beschwerdeführerin eingereichten Belege mit den Belegen einer anderen Beihilfeberechtigten vermischt wurden. Diese andere Beihilfeberechtigte, die dann die Belege der Beschwerdeführerin erhalten hatte, war bei der Polizeidienststelle beschäftigt. Als die fehlerhafte Versendung der Belege erkannt worden war, forderte die Beihilfestelle die Rücksendung der Belege. Hierzu nutzte die Beihilfeberechtigte keinen Briefumschlag, sondern den Faxanschluss ihrer Dienststelle. Die gefaxten Dokumente, die bei der Beihilfestelle wieder ankamen, trugen also den Fax-Absendevermerk der Polizeidienststelle. Die Beihilfestelle teilte mit, sie habe sich für den Fehler bei der Beschwerdeführerin bereits entschuldigt und die Bediensteten der Beihilfestelle nochmals zum Umgang mit den Unterlagen belehrt. Mit dem zuständigen Bediensteten, dem der Fehler unterlaufen war, wurde die Angelegenheit erörtert und ausgewertet. Damit waren geeignete Maßnahmen getroffen, um zukünftig die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen.

Da der Beschwerdeführerin nur die Faxausdrucke zugeleitet worden waren, stand die Frage im Raum, was denn mit den Originalbelegen passiert sei. Auf weitere Nachfrage des TLfDI teilte die Beihilfestelle mit, die andere Beihilfeberechtigte habe glaubhaft versichert, sie habe die Belege nach der Nutzung des Faxgeräts vernichtet. Die Beihilfestelle kam auch der Forderung des TLfDI nach, die andere Beihilfeberechtigte darauf hinzuweisen, dass es sich bei den Belegen der Beschwerdeführerin um besonders geschützte personenbezogene Daten im Sinne des § 4 Abs. 5 Thüringer Datenschutzgesetz handelte und diese keinesfalls durch sie genutzt werden dürfen.

Wird festgestellt, dass Unterlagen mit besonders geschützten personenbezogenen Daten an einen falschen Adressaten übersandt worden sind, müssen alle erforderlichen Maßnahmen getroffen werden, um die Belege im Original zurückzuerhalten. Der falsche Adressat ist auch darauf hinzuweisen, dass die zu schützenden personenbezogenen Daten keinesfalls genutzt werden dürfen.

11.14 Schließung eines Krankenhauses – Infektionsgefahr für Patientendaten? – Zur ordnungsgemäßen Archivierung

Aus einem Zeitungsartikel erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass eine Klinik beabsichtige, eines ihrer Krankenhäuser zu schließen. Bei der Schließung eines Krankenhauses stellt sich immer die Frage, was mit den Patientendaten passieren soll. Dies betrifft sowohl die Patientenakten aus Papier als auch die Patientendaten, die elektronisch gespeichert sind sowie die Informationstechnik des Krankenhauses selbst. Der TLfDI wandte sich an die verantwortliche Klinik und teilte dieser mit, dass sie als verantwortliche Stelle nach § 57 Abs. 10 Thüringer Krankenhausgesetz die technischen und organisatorischen Maßnahmen zu treffen habe, die erforderlich und angemessen sind, um die Beachtung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Hierzu gehören die Einhaltungen der Löschfristen und auch die Gewährleistung der Patientenrechte auf Auskunftserteilung nach dem Thüringer Krankenhausgesetz.
Die Klinik übersandte dem TLfDI ihre Archivordnung, die auch für die Akten des zu schließenden Krankenhauses zur Anwendung kommen sollte. Nach datenschutzrechtlicher Prüfung stellte der TLfDI fest, dass die dort enthaltenen Regelungen etwas zu allgemein gefasst waren. Es war nicht ganz eindeutig geregelt, in welchen Fällen und unter welchen Voraussetzungen Krankenhausakten an Dritte herausgegeben werden dürfen. Der TLfDI forderte, sicherzustellen, dass Arztpraxen Patientenakten nur dann erhalten dürfen, wenn eine Schweigepflichtsentbindung des Patienten vorliegt und an Forschungseinrichtungen prinzipiell nur anonymisierte Daten herauszugeben sind. Es existierten zudem keine klaren Regelungen zur Vernichtung von Patientenakten, in denen festgeschrieben wird, wer diese Akten wann vernichtet, durch wen dies protokolliert wird und welche Geräte zum Einsatz kommen. Weiterhin entsprach die Archivordnung nicht der geltenden Gesetzeslage im Hinblick auf das im Jahr 2013 in Kraft gesetzte Patientenrechtegesetz, das neue Regelungen im Bürgerlichen Gesetzbuch (BGB) trifft. Nach § 630g BGB ist dem Patienten auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist dabei zu begründen. Diese Voraussetzungen erfüllte

die Archivordnung nicht, da die Einsichtnahme pauschal verweigert wurde, wenn es um subjektive Wertungen, persönliche Bemerkungen oder Eindrücke des Arztes ging.
Weiterhin teilte die Klinik mit, dass bezüglich der Patientenakten des geschlossenen Krankenhauses im Klinikgebäude ein separater Archivraum genutzt würde. Die Einlagerung der Akten sei notwendig, da die Daten weiter aufbewahrt werden müssen, weil die Aufbewahrungsfristen noch nicht abgelaufen sind. Dokumente, die entsorgt werden durften, wurden nach Angaben der Ansprechpartner im Rahmen einer Auftragsdatenverarbeitung datenschutzgerecht vernichtet.
Die Archivordnung legte aber nicht fest, wie die Patientenakten der verschiedenen Kliniken jeweils getrennt aufbewahrt und vor dem Zugriff Unberechtigter geschützt werden sollten. Die Klinik wurde daher gebeten, die Archivordnung in allen durch den TLfDI kritisierten Punkten zu überarbeiten.
Die Klinik nahm daraufhin die notwendigen Änderungen ihrer Archivordnung vor und übermittelte sie erneut dem TLfDI zur Prüfung. Damit wurde dem größten Teil der Forderung des TLfDI nachgekommen. Einige unklare Punkte, wie beispielsweise die Frage, was mit den Personalakten der damals angestellten Mitarbeiter nach Auflösung des Krankenhauses passiert, konnten im weiteren Schriftverkehr geklärt werden.

Der TLfDI geht möglichen datenschutzrechtlichen Problemen nach, von denen er aus der Presse erfährt. Wird ein Krankenhaus geschlossen, muss es Festlegungen zum Umgang mit den dort vorhandenen personenbezogenen Daten (Patientendaten und Personaldaten) geben, die den datenschutzrechtlichen Bestimmungen entsprechen.

11.15 Darf der Hausarzt alles wissen?

Der Tag der offenen Tür des Thüringer Landtags, bei dem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) regelmäßig mit einem Stand vertreten ist, wird von Betroffenen auch genutzt, um ihre Beschwerden vorzubringen. Ein Betroffener wandte sich 2015 bei diesem Anlass an den TLfDI, um über Folgendes zu berichten: Das Universitätsklinikum Jena tausche Patientendaten mit den behandelnden Hausärzten aus. Der Beschwerdeführer sei im Klinikum behandelt worden. Als er dann zur

Nachbehandlung zu seinem Hausarzt gegangen sei, habe der schon alle seine Behandlungsdaten auf dem Bildschirm gehabt. Der Betroffene bat den TLfDI, den Sachverhalt zu überprüfen.
Da das Universitätsklinikum Jena als Krankenhaus mit anderen, auch privaten Krankenhäusern im Wettbewerb steht, gilt nach § 26 Thüringer Datenschutzgesetz grundsätzlich das Bundesdatenschutzgesetz (BDSG). Der TLfDI wies gegenüber dem Universitätsklinikum Jena darauf hin, dass ein solcher Austausch von besonderen Arten von personenbezogenen Daten, § 3 Abs. 9 BDSG, nur mit einer wirksamen Einwilligung des Betroffenen und unter Beachtung der nach § 9 BDSG erforderlichen Maßnahmen zulässig sei. Deshalb wurde erfragt, ob es schriftliche Festlegungen zu dem Verfahren gebe, in denen geregelt ist, ob und auf welche Weise die Einwilligung der betroffenen Patienten eingeholt werde, auf welche Weise genau die Datenübermittlung erfolge, welche Patientendaten auf welche Weise an welchem Ort für welche Zeit gespeichert würden und welche Personen unter welchen Voraussetzungen Zugriff auf diese Daten haben.
Die Klinik teilte mit, dass seit 2011 ein Zuweiserportal für niedergelassene Ärzte eingesetzt werde. Derzeit nutzen dieses Portal ausschließlich niedergelassene Ärzte der Fachrichtungen Urologie und Gynäkologie. Im Rahmen des Aufnahmeprozesses wird der Patient über die Möglichkeit der Nutzung dieses Portals aufgeklärt, wenn der angegebene niedergelassene Arzt an dem Verfahren teilnimmt. Der Patient hat dann die Wahl zu entscheiden, ob die Datenübermittlung an seinen Hausarzt beziehungsweise seinen weiterbehandelnden Arzt klassisch mit Papierversand oder über das Zuweiserportal erfolgen soll. Bei der Nutzung des Zuweiserportals erhält der Patient ein zusätzliches Informationsblatt zur Erläuterung des Verfahrens. Erst nach erfolgter schriftlicher Einwilligung erfolgt die Übermittlung an den (Haus-) Arzt.
Ob der Beschwerdeführer im vorliegenden Fall eine solche Einwilligung erteilt hatte, konnte vom TLfDI nicht geprüft werden, weil dieser Patient gegenüber dem TLfDI anonym bleiben wollte. Da der TLfDI der Sache aber grundsätzliche Bedeutung beimaß, wurden die technischen und organisatorischen Maßnahmen, die in Bezug auf das Projekt seitens des Klinikums nach § 9 BDSG getroffen wurden, vor Ort geprüft. Im Ergebnis wurde festgestellt, dass das Verfahren datenschutzkonform durchgeführt wurde. Für die Übermittlung ist eine rechtswirksame Einwilligung der Patienten Bedingung. Die wirksa-

me Einwilligung setzt nach § 4a BDSG voraus, dass sie auf der freien Entscheidung des Betroffenen beruht. Diese Voraussetzungen lagen vor, weil der Papierversand weiterhin als Alternative bestand und die Patienten in hinreichender Weise über das Verfahren aufgeklärt wurden. Es wurde im Rollen- und Berechtigungskonzept sichergestellt, dass nur berechtigte Ärzte auf die Daten Zugriff haben, die sie für die Weiterbehandlung ihres Patienten benötigen. Es lag eine hinreichende Verschlüsselung bei der Datenübertragung vor.

Eine Datenübermittlung durch das Krankenhaus ist nur mit schriftlicher Einwilligung des Patienten möglich. Das Krankenhaus muss mittels technischer und organisatorischer Maßnahmen sicherstellen, dass nur berechtigte Ärzte auf die Daten Zugriff haben, die sie für die Weiterbehandlung ihres Patienten benötigen. Dies war im vorliegenden Fall erfüllt.

11.16 Vernichtung von Patientendaten – gut gemeint, aber ...

Im Rahmen einer Vorortkontrolle bei einem Arzt brachte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfahrung, dass viele Ärzte in Thüringen ihre Patientenakten, die der gesetzlichen Aufbewahrungsfrist nicht mehr unterliegen, an die Kassenärztliche Vereinigung (KV) Thüringen zur Vernichtung weitergeben. Hierzu wurde die KV Thüringen um Abgabe einer Stellungnahme gebeten. Die KV Thüringen teilte mit, dass es sich um einen Service der KV handele, der allen knapp 4.000 Mitgliedern in Thüringen angeboten werde. Der Ablauf stellte sich dabei wie folgt dar:
Die Praxen vereinbaren mit der KV Thüringen einen Abholtermin, an dem ein datenschutzbelehrter Fahrer die Unterlagen in einem verschlossenen Behälter von der Praxis übernimmt. Die vollen Behälter werden dann bei der KV Thüringen zwischengelagert, in Behälter umgepackt, die von dem privaten Vernichtungsunternehmen zur Verfügung gestellt wurden. In diesen Behältern holt das Unternehmen die Akten dann in einem verschlossenen LKW ab und führt sie der weiteren Vernichtung zu. Das Verfahren wird dadurch protokolliert, dass die jeweiligen Behälter nummeriert werden und die Menge der übernommenen Behälter vom jeweiligen Fahrer quittiert wird.

Der TLfDI sah diesen Service durchaus kritisch. Nach § 203 Strafgesetzbuch macht sich strafbar, wer als Arzt unbefugt ein fremdes Geheimnis offenbart, das ihm in dieser Eigenschaft anvertraut worden ist. Nach der ersten Schilderung des Verfahrens war nicht ausgeschlossen, dass sowohl die Mitarbeiter der KV Thüringen als auch die Mitarbeiter des beauftragten Dienstleisters Patientendaten zur Kenntnis nehmen konnten. Auch eine Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG) reicht allein als Übermittlungsbefugnis in diesem sensiblen Bereich nicht aus. Vielmehr bedarf es einer Schweigepflichtsentbindungserklärung für das Verhältnis mit dem Auftragsdatenverarbeitungsnehmer, wenn tatsächlich Patientendaten offenbart werden. Mit der KV Thüringen wurde in einem Gespräch eine mögliche Vorgehensweise zur Vernichtung der Patientenakten besprochen. Nach Auffassung des TLfDI müssen die Daten von der KV Thüringen in einem verschlossenen Behältnis bei den Ärzten abgeholt werden. Die Ärzte müssen die Behältnisse selbst füllen und, wenn die Behältnisse nicht bereits verschlossen sind, verschließen. Die Behältnisse dürfen beim Transport und bei der KV Thüringen nicht geöffnet werden, sondern müssen verschlossen an den Dienstleister übergeben werden. In einem Vertrag mit dem Dienstleister muss festgelegt werden, wie dort mit den Daten zu verfahren ist und wie lange diese dort ggf. sicher aufbewahrt werden, bevor sie der Vernichtung zuzuführen sind. Für die Auswahl des Einsatzes von Aktenvernichtungsgeräten ist der erhöhte Vertraulichkeitsgrad der Dokumente ausschlaggebend. Nach Auffassung des TLfDI sind diese Dokumente, da sie einem Berufsgeheimnis unterliegen, mit Aktenvernichtungsgeräten zu schreddern, die nach der alten DIN-Norm 32757 mindestens die Sicherheitsstufe 4 oder nach der neuen DIN-Norm 663399-1 mindestens die Sicherheitsstufe P-5 aufweisen. Die KV Thüringen überarbeitete daraufhin die vorgesehenen Abläufe und reichte die überarbeiteten Unterlagen zur Prüfung ein. Leider konnte das Verfahren auch nach der überarbeiteten Prozessbeschreibung seitens des TLfDI nicht gutgeheißen werden. In den eingereichten Unterlagen war bei der Prozessbeschreibung der Aktenvernichtung ein Arbeitsschritt „Öffnen der Tonnen und Sichten des Inhalts“ vom privaten Dienstleister angegeben. Damit erhalten die Mitarbeiter des Dienstleisters Kenntnis vom Inhalt der Patientenunterlagen und die Aktenvernichtung ist aus den oben dargelegten Gründen datenschutzrechtlich nicht zulässig. Eine Offenbarung der dem Berufsgeheimnis unterliegenden Patientendaten liegt nur dann

nicht vor, wenn sichergestellt werden kann, dass jede Zugriffsmöglichkeit des beauftragten Dienstleisters auf die Daten ausgeschlossen werden kann. Dies kann nur durch verplombte bzw. versiegelte Umverpackungen (Kartonagen, Umschläge, Datentonnen) ausgeschlossen werden, die maschinell geöffnet und vernichtet werden. Die KV Thüringen wurde daher gebeten, die Vernichtung von Patientendaten über einen Dienstleister entweder einzustellen oder eine datenschutzgerechte Lösung zu finden, bei der sichergestellt ist, dass die Mitarbeiter des Dienstleisters nicht auf die Patientendaten zugreifen können. Daraufhin änderte die KV Thüringen das Verfahren erneut ab und reichte die geänderten Unterlagen nochmals dem TLfDI zur Prüfung ein. Diese Prüfung konnte im Berichtszeitraum noch nicht abgeschlossen werden, der Ausgang des Verfahrens bleibt abzuwarten. Der TLfDI ist mit Blick auf die bisherige Kooperation mit der KV Thüringen jedoch zuversichtlich.

Bei der Vernichtung von Patientenakten ist besondere Vorsicht geboten. Diese Daten unterliegen dem Berufsgeheimnis der Ärzte. Eine Offenbarung der einem Berufsgeheimnis unterliegenden Patientendaten liegt nur dann nicht vor, wenn sichergestellt werden kann, dass jede Zugriffsmöglichkeit des beauftragten Dienstleisters auf die Daten ausgeschlossen werden kann.

11.17 Überlassung von Patientenakten an ein Archiv im Sinne des Thüringer Archivgesetzes?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein Schreiben des Universitätsklinikums Jena (UKJ), das folgende zwei Fragen beantwortet haben wollte: Sind gemäß § 2 Abs. 1 Thüringer Archivgesetz (ThürArchivG) Patientenunterlagen eines Krankenhauses „archivwürdige Unterlagen“? Ist das Thüringer Archivgesetz aufgrund des § 20 Abs. 3 Thüringer Archivgesetz auf das UKJ überhaupt anwendbar? In seinem Schreiben wies das UKJ den TLfDI darauf hin, dass es unter anderem die gesetzliche Aufgabe der Krankenhausversorgung wahrnehme und es dazu im Wettbewerb mit den umliegenden Krankenhäusern im Freistaat Thüringen stehe.
Unter der Prämisse, dass die Überlassung von Patientenakten an ein Archiv im Sinne des ThürArchivG stets auch die Übermittlung per-

sonenbezogener Daten beinhaltet, beantwortete der TLfDI die beiden Fragen des UKJ wie folgt:
Patientenunterlagen des UKJ stellten nach Auffassung des TLfDI keine archivwürdigen Unterlagen gemäß § 2 Abs. 1 ThürArchivG dar. Dies ergab sich für den TLfDI aus folgenden Überlegungen:
§ 2 Abs. 1 ThürArchivG bestimmt, dass öffentliches Archivgut alle archivwürdigen Unterlagen der in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen sind, die zur dauernden Aufbewahrung von einem öffentlichen Archiv übernommen werden. Gem. § 3 Abs. 1 Satz 1 ThürArchivG werden als öffentliches Archivgut des Landes alle archivwürdigen Unterlagen bestimmt, die […] bei sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts entstanden sind und von den thüringischen Staatsarchiven nach Maßgabe dieses Gesetzes archiviert werden.
Diese Voraussetzungen des § 3 Abs. 1 Satz 1 ThürArchivG erfüllte das UKJ im zu beurteilenden Sachverhalt gerade nicht. Das UKJ ist zwar gemäß § 91 Abs. 1 Satz 1 Thüringer Hochschulgesetz (ThürHG) eine rechtsfähige Teilkörperschaft der Friedrich-Schiller-Universität Jena. Ferner untersteht das UKJ gemäß § 91 Abs. 4 1. Halbsatz ThürHG der Rechtsaufsicht des Landes.
Allerdings scheiterte eine Subsumtion des UKJ unter den § 3 Abs. 1 Satz 1 ThürArchivG daran, dass seine Unterlagen nicht nach Maßgabe dieses Gesetzes – dem ThürArchivG – zu archivieren sind. Dies ergab sich für den TLfDI daraus, dass das ThürArchivG gemäß § 20 Nr. 3 ThürArchivG nicht für öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit gilt, die am wirtschaftlichen Wettbewerb teilnehmen, und für deren Zusammenschlüsse. Im genannten Schreiben des UKJ wies dies aber gerade darauf hin, dass es für den Bereich der Krankenversorgung im Wettbewerb mit umliegenden Krankenhäusern im Freistaat Thüringen stehe. Dem TLfDI waren auch keine anderen Sachverhalte bekannt, die an einer Teilnahme des UKJ am wirtschaftlichen Wettbewerb Zweifel begründeten. Deshalb lag nach Auffassung des TLfDI hier der Ausschlussgrund des § 20 Nr. 3 ThürArchivG für dessen Anwendbarkeit auf Patientenunterlagen des UKJ vor. Folglich stellten die Patientenakten auch kein Archivgut im Sinne des § 3 Abs. 1 ThürArchivG dar.
Damit war zugleich auch die zweite Frage des UKJ beantwortet, ob das ThürArchivG aufgrund von § 20 Abs. 3 ThürArchivG überhaupt anwendbar sei.

Gegen diese Rechtsauffassung des TLfDI zeichnete sich ganz zum Ende des Berichtszeitraums jedoch Widerspruch aus dem Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) ab. Konkret zweifelte das TMWWDG daran, dass das UKJ am wirtschaftlichen Wettbewerb im Sinne von § 20 Abs. 3 ThürArchivG teilnehme. Der TLfDI forderte deshalb das TMWWDG auf, seine Rechtsauffassung zu begründen. Da diese Stellungnahme aus dem TMWWDG zu Redaktionsschluss noch nicht vorlag, wird der TLfDI im nächsten Tätigkeitsbericht über den Fortgang dieses Verfahrens informieren.

Der Umgang mit öffentlichem Archivgut und der Schutz personenbezogener Daten haben immer wieder Schnittmengen zur Folge, die dann der TLfDI datenschutzrechtlich bewerten muss: Wenn personenbezogene Daten in Patientenakten enthalten sind, stellt sich die Frage, ob und wie diese zu schützen sind und ob Krankenhäuser als öffentliche Stellen verpflichtet sind, diese Akten den öffentlichen Archiven gemäß § 11 Abs. 1 Satz 1 ThürArchivG anzubieten. Hier ist insbesondere § 20 Abs. 3 ThürArchivG zu beachten, der bestimmt, dass das ThürArchivG dann nicht gilt, wenn öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit am wirtschaftlichen Wettbewerb teilnehmen. Ob diese Tatbestandsvoraussetzungen vorliegen, hat der TLfDI in jedem Fall durch Prüfung zu ermitteln.

11.18 Die Thüringer Krankenhäuser – Heilung in Sicht

Bereits im 9. und 10. Tätigkeitsbericht zum Datenschutz im öffentlichen Bereich berichtete der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über die Orientierungshilfe „Krankenhausinformationssysteme“ (OH KIS). Wie im letzten Tätigkeitsbericht angekündigt, wurde diese aus rechtlicher und technischer Sicht aktualisiert und steht nunmehr seit März 2014 auf den Seiten des TLfDI in ihrer neuen Fassung bereit unter: https://www.tlfdi.de/imperia/md/content/datenschutz/themen/gesundheit/oh_kis_v2_korr.pdf

Die OH KIS richtet sich nicht nur an die Krankenhausbetreiber und Hersteller von Krankenhausinformationssystemen, sondern bildet auch die Grundlage für datenschutzrechtliche Kontrollen der Aufsichtsbehörden des Bundes und der Länder. Auch der TLfDI richtet sich bei seinen Kontrollen nach der OH KIS.
Das Spektrum der festgestellten Mängel ist dabei vielfältig: vom Fehlen konkreter Regelungen zu datenschutzrelevanten Themen, wie Umgang mit Dienst-E-Mail-Zugängen oder den Zugriff auf Patientendaten im Notfall, bis zu unzulässigen Regelungen zur Passwortverwendung und -gültigkeit.
Ein Krankenhaus bearbeitet ein komplexes Feld an Vorgängen, die täglich anfallen. Unter diesen Vorgängen stachen vor allen Dingen einige Probleme hervor, die regelmäßig in vielen Krankenhäusern auftraten. So war zu beobachten, dass sowohl die Ärzte, die Pfleger wie auch das Kostenabrechnungspersonal sehr weitgehende Rechte zur Einsicht in die elektronische Patientenakte hatten. Hier forderte der TLfDI eine Überarbeitung der Zugriffsrechte. Ärzte und Pflegepersonal dürfen grundsätzlich nur auf Patientenakten zugreifen, an deren Behandlung sie auch beteiligt sind. Zu weit reichende Zugriffsrechte können einen Verstoß gegen § 203 Strafgesetzbuch (ärztliche Schweigepflicht) darstellen. Beim Abrechnungspersonal ist die Lage bezüglich der Notwendigkeit der Zugriffe komplizierter – hier ist der TLfDI noch in Diskussion mit den Krankenhäusern. Insgesamt dauert die Umstellung der Zugriffsrechte in den Krankenhäusern noch an, wurde aber durch die Kontrolle des TLfDI angestoßen. Hier muss insbesondere die Gesundheit der Patienten im Vordergrund stehen, was allerdings keinen Freibrief für einen umfassenden Zugriff aller Ärzte darstellt. Eine Möglichkeit der Sicherstellung sowohl der Patientensicherheit als auch der datenschutzgerechten Zugriffe auf Patientendaten ist der so genannte Notfallzugriff. Hier kann der Arzt sich über bestehende Zugriffsschranken hinwegsetzen und die Daten dennoch einsehen. Um dies zu tun, muss er allerdings eine Begründung im System hinterlegen, und der Zugriff muss protokolliert werden. Auch dieser Punkt ist noch nicht in allen Krankenhäusern abschließend umgesetzt. So fordert die oben genannte Orientierungshilfe auch insgesamt eine umfassende Protokollierung der Zugriffe auf Patientendaten und deren regelmäßige, stichprobenhafte oder anlassbezogene Auswertung, um Missbrauch zu erschweren. Oft setzt hier die eingesetzte Software dem Krankenhaus Schranken, und die Softwareanbieter sind hier in der Pflicht,

ihre Software entsprechend den datenschutzrechtlichen Anforderungen anzupassen – ein nicht unerheblicher Aufwand und häufig auch Neuland für die Kliniken und Softwarehersteller.
Gleichfalls gibt es von den Softwareherstellern verursachte, ganz grundlegende Probleme. So sind z. B. in den derzeit sechs kontrollierten Krankenhäusern fünf verschiedene Krankenhausinformationssysteme im Einsatz, wobei nur eines dieser Systeme in der Lage ist, Daten entsprechend den gesetzlich vorgeschriebenen Löschfristen auch tatsächlich zu löschen. So fordert der Gesetzgeber beispielsweise, dass Patientendaten nach spätestens 30 Jahren (für einige Daten auch weniger) gelöscht oder anonymisiert werden müssen. Meist besteht die Möglichkeit, Daten zu sperren, um sie vor unberechtigtem Zugriff zu schützen, aber auch dieser Vorgang ist umständlich und noch nicht im notwendigen Maß automatisiert. Auch an dieser Stelle haben die Softwarehersteller in den nächsten Jahren noch Nachholbedarf, die Sperrfunktion im benötigten Umfang komfortabel und datenschutzrechtskonform in ihre Systeme zu integrieren.
Viele organisatorische Mängel konnten bereits beseitigt werden. Die Krankenhäuser sind sich der datenschutzrechtlichen Situation bewusst und sehr kooperativ. Der TLfDI wird entsprechend seiner Kontrollkompetenz weiterhin die Umsetzung der OH KIS fordern und deren datenschutzgerechte Umsetzung beobachten. Heilung ist in Sicht.

Gesundheitsdaten sind sensible personenbezogene Daten. Die Orientierungshilfe Krankenhausinformationssysteme bildet dabei eine gute Grundlage, Krankenhausinformationssysteme datenschutzgerechter zu gestalten und einzusetzen. Die stichpunktartigen Kontrollen ergaben bisher, dass dies aber ein zäher Prozess sowohl bei den Krankenhausbetreibern als auch bei den Herstellern von Krankenhausinformationssystemen ist.

11.19 AlertsNet: Bei Keimen im Blut fließen Daten gut!

Krankenhauskeime sind zunehmend eine echte Gefahr für Patienten, Angestellte und Besucher der Kliniken. Die Übersicht zu behalten, in welchen Stationen welche Keime auftreten, ist nicht immer einfach. Daher ist eine genaue Überwachung dieser Patienten wichtig, wenn ihre Infektion einmal erkannt wurde. Außerdem ist eine statistische Auswertung zur Qualitätssicherung, in welchen Teilen der Kliniken

welche Erreger vorkommen, für das Hygienemanagement der Klinik von Bedeutung. Auch der Vergleich zu anderen Kliniken ist hier für das Qualitätsmanagement der jeweiligen Klinik wichtig.
Das Projekt „AlertsNet“ des Universitätsklinikums Jena erfasst dazu thüringenweit Daten zu auftretenden Fällen von Krankenhauskeimen im Blut. Erhoben werden zum einen Laborbefunde von Blutuntersuchungen, die zuvor von den Laboren als infiziert eingestuft wurden. Im zweiten Schritt werden dann vom Universitätsklinikum zusätzliche Daten zum Betroffenen abgefragt, wie z. B. Name, Vorname, Geburtsdatum, Geschlecht, Krankenhausstation, Behandlungsfokus, Risikofaktoren wie Katheter oder Kanülen, Entlassungsstatus und Schweregrad der Infektion. AlertsNet will neben dem Erfassen von Diagnosen und deren statistischen Auswertungen auch Behandlungshinweise an die entsprechenden Ärzte geben. Ziel ist dabei, auch selten auftretende Infektionen durch das Expertenteam optimal zentral versorgen zu können.
Das System erhebt Gesundheitsdaten und damit besondere Arten von Daten, die vom Gesetz besonders geschützt sind, § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG). Auf das Universitätsklinikum Jena ist im vorliegenden Fall das BDSG anzuwenden, weil es als Krankenhaus am Wettbewerb teilnimmt, § 26 Thüringer Datenschutzgesetz. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nach § 4 Abs. 1 BDSG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Die Datenerfassung basiert mangels Rechtsgrundlage auf der Einwilligung der betroffenen Person (Patient oder Angestellter). An die Einwilligung sind wegen der Verarbeitung von Gesundheitsdaten hohe Anforderungen zu stellen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform. Da besondere Arten personenbezogener Daten erhoben und verarbeitet werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG.
Im Rahmen dieses Forschungsprojektes wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) um Stellungnahme zur Einwilligungserklärung sowie zu den Sicherheits- und Anonymisierungsmaßnahmen gebeten. Der TLfDI

wirkte darauf hin, dass die Einwilligungserklärung den gesetzlichen Anforderungen genügte. Im Hinblick auf die Sicherheits- und Anonymisierungsmaßnahmen sieht der TLfDI zwischen den Problemstellungen „statistische Auswertung“ und „Behandlungsvorschläge“ ein gewisses Spannungsfeld. Um nach der ersten Diagnose durch ein Labor auch alle weiteren Daten zu erfassen, muss dem System die betroffene Person zur korrekten Zuordnung bekannt sein. Ebenso muss auch für die Behandlungsvorschläge ein Ansprechpartner bekannt sein. Die Daten werden dazu pseudonymisiert in einer Datenbank gespeichert. Für die statistische Auswertung ist dagegen kein Personenbezug mehr notwendig. Dies bedeutet, dass der Personenbezug aus den gespeicherten Daten gelöscht werden muss, wenn er nicht mehr erforderlich ist. Da für die Nacherfassung und den Behandlungsvorschlag der sinnvoll nutzbare Zeitraum begrenzt ist, werden die personenbezogenen Daten nach sechs Wochen aus der Datenbank gelöscht und liegen dann nur noch in anonymisierter Form zur statistischen Auswertung und Qualitätskontrolle vor. Außerdem prüfte der TLfDI die technischen und organisatorischen Maßnahmen zum Schutz der Datenbank. Hier konnten keine Mängel festgestellt werden.

Die Datenerfassung bei dem Forschungsprojekt AlertsNet beruht auf Einwilligungsbasis. Die übermittelten Daten werden nach Ablauf von sechs Wochen anonymisiert. Das Forschungsprojekt hat frühzeitig die Philosophie der Datensparsamkeit gewählt und diese dadurch in der Programmierung der Software schon mit berücksichtigt.

11.20 Datenschutz vs. Auskunftsrecht

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Landesärztekammer Thüringen ihm eine Auskunft verweigere. Er hatte sich mit einer Beschwerde über einen Arzt dort gemeldet und wollte jetzt wissen, wie der Ausgang des Verfahrens war. Die Landesärztekammer teilte ihm mit, dass er aus Datenschutzgründen keine Auskunft erhalten werde.
Vor längerer Zeit hatte sich die Landesärztekammer Thüringen aufgrund der Beschwerde eines Rechtsanwaltes eines Arztes intensiv mit der Fragestellung befasst, welche Informationen ein Beschwerdeführer im Rahmen eines berufsrechtlichen Verfahrens erhalten

darf. In diesem Zusammenhang hatte sich die Kammer auch an den TLfDI gewandt. Die datenschutzrechtliche Prüfung des TLfDI hatte zum Ergebnis, dass das berufsrechtliche Verfahren nach dem Thüringer Heilberufegesetz (ThürHeilBG) als kammerinternes Verfahren ausgestaltet ist und eine Rechtsgrundlage für eine Information an den Beschwerdeführer nicht gegeben ist. Nach § 4 Abs. 1 Thüringer Datenschutzgesetz bedarf nämlich eine Datenübermittlung an den Beschwerdeführer entweder einer gesetzlichen Vorschrift oder der Einwilligung des Betroffenen. Daher kann der Beschwerdeführer lediglich über den Verfahrensstand informiert werden, eine Mitteilung des Ergebnisses des berufsrechtlichen Verfahrens muss aus datenschutzrechtlichen Gründen unterbleiben. Diese Auffassung wird auch von der Rechtsprechung bestätigt. So hat das OVG Lüneburg mit Beschluss vom 29. Januar 2008, Az.: 11 LA 448/07, ausdrücklich festgestellt, dass der Beschwerdeführer nur darüber unterrichtet wird, dass eine berufsrechtliche Prüfung stattfindet.
Die Landesärztekammer hatte daher zu Recht auf den Datenschutz verwiesen. Dies wurde dem Beschwerdeführer mitgeteilt.

In berufsrechtlichen Verfahren nach dem ThüHeilBG hat derjenige, der das Verfahren durch seine Beschwerde angestoßen hatte, nur Anspruch auf die Auskunft, dass eine berufsrechtliche Prüfung stattfindet, nicht aber auf das Ergebnis der Prüfung.

11.21 Datenerhebung der Gemeinsamen Prüfungseinrichtung bei Thüringer Ärzten

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass die Gemeinsame Prüfungseinrichtung der Ärzte und Krankenkassen in Thüringen die Übermittlung von Diagnosen und weiterer Angaben zu Krankheiten verlangt, wenn an Ärzte Prüfaufträge gerichtet werden. Die Erhebung dieser Daten seitens der Gemeinsamen Prüfungseinrichtung erfasste dabei auch Gesundheitsdaten der Patienten. Der TLfDI wandte sich an die Gemeinsame Prüfeinrichtung und bat diese, mitzuteilen, auf welcher Rechtsgrundlage diese Datenerhebung erfolgte und welche technisch-organisatorischen Maßnahmen zum Schutz dieser Daten getroffen worden sind.
Die Gemeinsame Prüfeinrichtung ließ wissen, dass die von Kassenärztlicher Vereinigung und Krankenkassen getragenen Prüfungsein-

richtungen (Prüfungsstelle und – für Widerspruchsverfahren – der Beschwerdeausschuss) den in § 106 Sozialgesetzbuch (SGB) Fünftes Buch (V) normierten Auftrag durch Beratungen und Prüfungen erfüllen. Die Wirtschaftlichkeitsprüfung der Vertragsärzte umfasse im Wesentlichen drei Konstellationen, die sich unmittelbar aus dem Gesetz ergäben:
Die Auffälligkeitsprüfung nach § 106 Abs. 2 Nr. 1 SGB V, die auf einer statistischen Überschreitung von Verordnungssummendaten beruht, die Zufälligkeitsprüfung nach § 106 Abs. 2 Nr. 2 SGB V, in die je Quartal zwei vom Hundert der Vertragsärzte für den Zeitraum von vier aufeinanderfolgenden Quartalen einbezogen werden sollen und die auf der Basis von arzt- und versichertenbezogenen Stichproben stattfindet sowie die Einzelfallprüfung nach § 106 Abs. 3 Satz 3 i. V. m. § 11 der Thüringer Prüfvereinbarung. In allen Konstellationen könne es möglich sein, dass die Prüfungsstelle oder auch der Beschwerdeausschuss Diagnosedaten oder weitere Begleitumstände ärztlicher Therapien zu den von einem Prüfverfahren Betroffenen abfordere oder hinterfrage. Die Diagnosedaten seien insbesondere für die Zufälligkeitsprüfung erforderlich, da hier gemäß § 106 Abs. 2a SGB V die medizinische Notwendigkeit ebenso zu beurteilen sei wie die Eignung der Behandlung zur Erreichung des therapeutischen Ziels. Ob eine ärztliche Leistung bzw. Verordnung angemessen, zweckmäßig und effektiv ist, lasse sich nur dann beurteilen, wenn die Indikation und damit auch die Diagnose feststehen.
lm Regelfall prüfe die Prüfungsstelle auf der Grundlage der von der Kassenärztlichen Vereinigung und den Krankenkassen übermittelten Daten. Nur in den Fällen, in denen die regelhaften Datenlieferungen Unklarheiten durch unsachgemäße oder ungenaue Kodierung von Diagnosen, fehlende Diagnosen oder sonstige Unplausibilität der Behandlung (Diagnose passt nicht zur Verordnung) erkennen ließen, fragten die Prüfgremien konkret den Arzt nach den patientenindividuellen Behandlungsumständen. Die Mitarbeiter der Prüfungsstelle seien ebenso wie die Mitglieder des Beschwerdeausschusses schriftlich zur Einhaltung des Datenschutzes verpflichtet. Es wurde eine Datenschutzdienstanweisung und eine IT-Sicherheitsrichtlinie übermittelt.
Der TLfDI wies in diesem Zusammenhang darauf hin, dass zwar die gesetzliche Regelung des § 106 SGB V i. V. m. §§ 296, 298 SGB V die Übermittelung von Versichertendaten durch kassenärztliche Vereinigungen bzw. die Krankenkassen vorsehe. Eine Übermitt-

lungsbefugnis der Ärzte an die Gemeinsame Prüfeinrichtung gebe es im Gesetz aber nicht. Auch der vorgelegten Prüfvereinbarung zwischen der kassenärztlichen Vereinigung Thüringen und den Landesverbänden der Krankenkassen konnte eine derartige Übermittlungsbefugnis bzw. -pflicht nicht entnommen werden. Die Gemeinsame Prüfeinrichtung wurde daher zunächst gebeten, künftig in Fällen, in denen die regelhaften Datenlieferungen der kassenärztlichen Vereinigung oder der Krankenkassen Unklarheiten durch unsachgemäße oder ungenaue Codierung von Diagnosen, fehlende Diagnosen oder sonstige Unplausibilitäten der Behandlung erkennen lassen, streng nach dem gesetzlich vorgesehenen Verfahren vorzugehen und diese Daten nur bei den kassenärztlichen Vereinigungen bzw. bei den Krankenkassen zu erheben. Der TLfDI bezog in die Prüfung mit ein, dass die Rechtsprechung (Urteil des LSG Nordrhein-Westfalen vom 14. Dezember 2011 [L11 KA 75/10]; Urteil des BSG vom 13. August 2014 [B 6 KA 41113 R]) eine besondere Mitwirkungspflicht des Vertragsarztes im Wirtschaftlichkeitsprüfverfahren postuliert hat. Außerdem sollte nach der Gesetzesbegründung (Bundestags-Drucksache 12/5187) klargestellt werden, dass der behandelnde Vertragsarzt verpflichtet ist, die im Rahmen von Prüfverfahren notwendigen Unterlagen mit versichertenbezogenen Angaben zu offenbaren und er insofern von seiner Schweigepflicht entbunden ist. Der Gesetzeswortlaut wurde rechtsprechungskonform ausgelegt. Danach bestand eine besondere Mitwirkungspflicht des Vertragsarztes im Wirtschaftlichkeitsprüfverfahren nach § 106 SGB V und der TLfDI sah die Angelegenheit als erledigt an.

Grundsätzlich dürfen auch bei Verfahren nach dem SGB Daten nur verarbeitet werden, wenn die einschlägige gesetzliche Ermächtigungsgrundlage dies vorsieht. Es kommt allerdings vor, dass bestimmte Verfahrensweisen, die sich aus dem Gesetz nicht eindeutig ergeben, durch die Rechtsprechung für zulässig erachtet werden, weil sie das Gesetz unter Berücksichtigung des Willens des Gesetzgebers auslegt.

11.22 Spender-Anamnesebogen für Angehörige von Organspendern

Ein Transplantationsbeauftragter bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um

Hilfe. Seine Aufgabe besteht beispielsweise darin, potentielle Organspender zu identifizieren, die Hirndiagnostik mit durchzuführen und die notwendigen Gespräche mit den Angehörigen im Falle einer Organspende zu führen. Der Transplantationsbeauftragte wünschte eine datenschutzrechtliche Überprüfung eines Spender-Anamnesebogens, der den Angehörigen des verstorbenen Organspenders mit der Bitte um Beantwortung vorgelegt wird. Dieser von der Deutschen Stiftung für Organtransplantation erstellte Spender-Anamnesebogen hat zum Ziel, anamnesische Angaben, also die gesundheitliche Vorgeschichte des Verstorbenen, durch die Befragung der Angehörigen zu erhalten. Wie der TLfDI bei der Prüfung des Bogens feststellen konnte, enthält dieser nicht nur gesundheitliche Fragen zum Organspender, sondern auch die Angabe, ob dieser einer Risikogruppe für AIDS und Hepatitis angehörte und falls ja, welcher. Im Ergebnis gelangte der TLfDI zur Überzeugung, dass sich im Hinblick auf die Anamnese sowie die Lebensumstände des verstorbenen Organspenders die datenschutzrechtlichen Interessen des Verstorbenen und seiner Angehörigen mit denjenigen des potenziellen Organempfängers, der ein schutzwürdiges Interesse daran hat, sein Gesundheitsrisiko durch den Erhalt des Spenderorganes möglichst gering zu halten, widerstritten. Hierbei ist zu berücksichtigen, dass sich Angehörige von Verstorbenen nach der Rechtsprechung nur in sehr geringem Maße auf deren Grundrecht auf informationelle Selbstbestimmung berufen können (siehe BVerfGE 30, 173 (196)). Zum anderen ist das Recht auf körperliche Unversehrtheit (Artikel 2 Abs. 2 des Grundgesetzes) derjenigen, die ein Spenderorgan erhalten sollen, hoch zu bewerten. Der TLfDI hat daher keine grundsätzlichen datenschutzrechtlichen Bedenken gesehen, wenn bestimmte Daten abgefragt werden, die erforderlich sind, um in Erfahrung zu bringen, ob das Spenderorgan für die Transplantation geeignet ist oder nicht.

Der Spender-Anamnesebogen, der den Angehörigen eines verstorbenen Organspenders zur Beantwortung vorgelegt wird, enthält eine Reihe von besonders schutzwürdigen Arten personenbezogener Daten sowohl hinsichtlich des Gesundheitszustandes als auch der ehemaligen Lebensumstände. Insgesamt überwiegt das Recht auf körperliche Unversehrtheit des möglichen Organempfängers das datenschutzrechtliche Interesse des Verstorbenen und seiner Angehörigen,

sodass gegen die Datenerhebung keine durchgreifenden Bedenken geltend gemacht werden.

11.23 ARMIN soll Patienten schützen

Für die AOK Plus ist eigentlich der Sächsische Datenschutzbeauftragte die zuständige Aufsichtsbehörde. Gleichwohl wandte sich die Krankenkasse an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Hintergrund war folgender:
Die Krankenkassen und ihre Verbände können im Rahmen ihrer gesetzlichen Aufgabenstellung zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung Modellvorhaben zur Weiterentwicklung der Verfahrens-, Organisations-, Finanzierungs- und Vergütungsformen der Leistungserbringung durchführen, § 63 Sozialgesetzbuch (SGB) Fünftes Buch (V). Die AOK Plus wollte das Modellprojekt „Arzneimittelinitiative Sachsen-Thüringen" (ARMIN) initiieren und band den TLfDI frühzeitig ein. Selbstverständlich stimmte sich der TLfDI auch mit dem Sächsischen Datenschutzbeauftragten ab.
Kern des Modells ist ein von Arzt und Apotheker gemeinsam durchgeführtes Medikationsmanagement für Versicherte dieser Krankenkasse, die von so genannter Multimedikation betroffen sind. Hiervon spricht man, wenn eine Vielzahl verschiedener Medikamente eingenommen werden muss. Zwar ist der TLfDI nicht für die datenschutzrechtliche Aufsicht über die AOK Plus zuständig, wohl aber für die Ärzte und Apotheken in Thüringen. Daher war auch eine Abstimmung mit dem TLfDI notwendig.
Das Modellprojekt sieht vor, einen elektronischen Medikationsplan mittels eines Medikationsplanservers bereitzustellen, der Transparenz über das Verordnungsgeschehen herstellt. Damit soll die Arzneimitteltherapiesicherheit verbessert werden. Es kann beispielsweise verhindert werden, dass zwei Ärzte Medikamente verschreiben, die sich nicht miteinander vertragen.
Nach Auffassung des TLfDI ist ein derartiges Projekt nur möglich, wenn eine wirksame Einwilligung des Patienten vorliegt. Nach § 4a BDSG ist der Betroffene auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist

außerdem nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung bedarf der Schriftform.
Der Versicherte entscheidet sich für die Betreuung durch einen an ARMIN teilnehmenden Arzt und eine an ARMIN teilnehmende Apotheke seiner Wahl. Die Teilnahme an ARMIN ist freiwillig. Teilnahmeberechtigt sind Versicherte der AOK PLUS, sofern sie das 18. Lebensjahr vollendet haben, mittels schriftlicher Erklärung in die Bedingungen des Vertrages einwilligen, nicht dauerhaft in Pflegeeinrichtungen stationär betreut werden und gleichzeitig eine Arzneimitteltherapie mit mindestens fünf Wirkstoffen erhalten.
Personenbezogene Daten werden im Rahmen des Medikationsmanagements dezentral beim behandelnden Arzt und Apotheker erhoben, gespeichert, verarbeitet und genutzt. Hierbei finden die Bestimmungen des Bundesdatenschutzgesetzes Anwendung. Die Einwilligungserklärung wurde mit dem TLfDI abgestimmt. Mit der Einwilligungserklärung räumt der Versicherte seinem gewählten Arzt und Apotheker Zugriff auf seine personenbezogenen Arzneimittelverordnungsdaten der letzten sechs Monate ein. Der Arzt und der Apotheker können diese Angaben nötigenfalls ergänzen, beispielsweise um bestimmte Unverträglichkeiten. Es können auch weitere verordnete Arzneimittel oder solche Mittel mit aufgenommen werden, die der Patient selbst erworben hat.
An dem Modellprojekt teilnehmende Ärzte und Apotheker verpflichten sich bei ihrer Teilnahme, bestimmte technische Mindestanforderungen zu erfüllen, welche neben der Sicherstellung der erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes einzuhalten sind. Hierzu zählt u. a. die Verwendung einer vertragskonformen Software. Dabei ist die Vertragskonformität mit einer Zertifizierung nachzuweisen. Mit der Einwilligung erlaubt der Teilnehmer dem Arzt und Apotheker untereinander den Austausch der für die Betreuung erforderlichen Medikationsdaten. Die Medikationspläne werden zwischen Arzt und Apotheker über einen extern gesicherten Server im Netz der Krankenversicherungen, über das bereits die ärztliche Abrechnung läuft, ausgetauscht. Die AOK PLUS kann nach ihren Angaben zu keinem Zeitpunkt die Daten auf dem Medikationsplanserver einsehen.
Der TLfDI wies darauf hin, dass der Versicherte nach § 34 BDSG gegenüber den Ärzten und Apothekern Auskunftsrechte zu den zu ihm gespeicherten personenbezogenen Daten innehat. Die Teilnahme

am Modellprojekt kann gegenüber der AOK PLUS auch wieder gekündigt werden.
Der TLfDI wird das Verfahren weiterhin gemeinsam mit dem Sächsischen Datenschutzbeauftragten begleiten und gegebenenfalls die Einhaltung der schriftlich fixierten Vorgaben vor Ort prüfen.

Wenn die Krankenkassen Modellvorhaben zur Verbesserung der Qualität und der Wirtschaftlichkeit der medizinischen Versorgung durchführen, betrifft dies oftmals auch die Verarbeitung personenbezogener Daten. Es ist ratsam die erforderlichen technischen und organisatorischen Maßnahmen frühzeitig mit dem TLfDI abzustimmen.

11.24 Einsichtnahme in Todesbescheinigungen für eine wissenschaftliche Studie

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom damaligen Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) gebeten, aus datenschutzrechtlicher Sicht zu einer im Universitätsklinikum der Friedrich-Schiller-Universität Jena durchgeführten Studie Stellung zu nehmen. Im Rahmen dieser Studie wollte das Universitätsklinikum die Todesursachen von verstorbenen Patienten, die zuvor an dieser Studie teilgenommen hatten, einer wissenschaftlichen Untersuchung unterziehen. Der TLfDI verwies in seiner Stellungnahme an das TMSFG auf § 15 Abs. 4 Thüringer Bestattungsgesetz (ThürBestG), in dem festgelegt ist, unter welchen Voraussetzungen die für den Wohnort des Verstorbenen zuständige untere Gesundheitsbehörde auf Antrag Auskünfte aus Totenscheinen erteilen kann. Sofern das TMSFG nach § 15 Abs. 4 Satz 1 Nr. 2 Buchstabe b) ThürBestG nicht feststellte, dass ein öffentliches Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, wofür nach dem Dafürhalten des TLfDI nach dem Vorbringen des Universitätsklinikums einiges sprach, kam nur der Erlaubnistatbestand des § 15 Abs. 4 Satz 1 Nr. 1 ThürBestG in Betracht. Danach kann der Antragsteller auf Antrag Auskunft aus Toten- und Sektionsscheinen bekommen, wenn er ein berechtigtes Interesse glaubhaft macht und kein Grund zu der Annahme besteht,

dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Angehörigen beeinträchtigt werden. Im vorliegenden Fall wurde nach Auffassung des TLfDI jedoch Auskunft aus einem wissenschaftlichen Interesse heraus begehrt. § 15 Abs. 4 Satz 1 Nr. 2 ThürBestG gestattet unter bestimmten Voraussetzungen die wissenschaftliche Auswertung der bei der für den Wohnort zuständigen unteren Gesundheitsbehörde verwahrten Daten. Die Verwendung von personenbezogenen Daten ohne sofortige Anonymisierung oder Pseudonymisierung bedarf auch nach der Gesetzesbegründung (Landtagsdrucksache 3/3937, S. 33 zu § 15) der Genehmigung des für das Gesundheitswesen zuständigen Ministeriums. Sie darf nur erteilt werden, wenn an dem Forschungsvorhaben ein erhebliches Interesse der Allgemeinheit besteht. Diese gesetzliche Voraussetzung sollte nicht durch eine Anwendung von § 15 Abs. 4 Nr. 1 ThürBestG umgangen werden. Ob die Voraussetzungen des § 15 Abs. 4 Satz 1 Nr. 2 Buchstabe b) ThürBestG vorlagen, unterlag letztlich der fachlichen Entscheidung durch das TMSFG.

Die Auskunft aus Toten- und Sektionsscheinen ist spezialgesetzlich in § 15 des Thüringer Bestattungsgesetzes geregelt. Entweder muss ein Antragsteller bei der für den Wohnort des Verstorbenen zuständigen Gesundheitsbehörde ein berechtigtes Interesse glaubhaft machen und es darf kein Grund zu der Annahme bestehen, dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Angehörigen beeinträchtigt werden, oder die Angaben werden für ein wissenschaftliches Vorhaben benötigt. In diesem Fall muss entweder durch sofortige Anonymisierung oder Pseudonymisierung der Angaben sichergestellt werden, dass schutzwürdige Belange des Verstorbenen und seiner Angehörigen nicht beeinträchtigt werden, oder das für das Gesundheitswesen zuständige Ministerium muss feststellen, dass das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Bei einem wissenschaftlichen Vorhaben sollte stets das hier zuständige Ministerium das Vorliegen eines überwiegenden öffentlichen Interesses prüfen und die Auskunft bzw. Einsicht letztlich auf dieser Grundlage erfolgen.

11.25 Grenzenlose Datenerhebung bei Einschulungsuntersuchungen des Kinder- und Jugendärztlichen Dienstes der Gesundheitsämter?

Das Thüringer Landesverwaltungsamt (TLVwA) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung, ob aus datenschutzrechtlicher Sicht im Rahmen der obligatorischen Einschulungsuntersuchung in Thüringen zukünftig zusätzlich der Parameter „Migrationshintergrund“ erhoben werden darf. Hierzu wurde dem TLfDI ein zum Thüringer Anamnese-Erhebungsbogen zur Einschulungsuntersuchung zusätzlicher Fragebogen zur Erfassung des Migrationshintergrunds vorgelegt, in dem beide Elternteile danach befragt werden, in welchem Land sie geboren wurden, welche Staatsangehörigkeit sie derzeit besitzen und ob ihr Kind in Deutschland geboren wurde. Der TLfDI hatte sich in der Vergangenheit aufgrund von Bürgereingaben bereits mit der Frage auseinandergesetzt, welche personenbezogenen Angaben über das einzuschulende Kind und dessen Eltern erfragt werden dürfen. Die hierbei einschlägigen Rechtsvorschriften enthalten weder einen Musterfragebogen noch einen abschließenden Datenkatalog. Der TLfDI hatte die datenschutzrechtliche Zulässigkeit einer Erweiterung des bisherigen Fragebogens um eine „einheitliche Erfassung des Migrationshintergrundes“ anhand der vorhandenen Rechtsvorschriften in diesem Bereich zu prüfen. Nach § 8 Abs. 1 der Thüringer Verordnung über die Schulgesundheitspflege (ThürSchulgespflVO) darf das Gesundheitsamt zur Erfüllung der ihm aufgrund dieser Verordnung zugewiesenen Aufgaben die dafür erforderlichen Daten verarbeiten und nutzen. Diese Aufgaben sind insbesondere in den in § 1 ThürSchulGespflVO aufgeführten Grundsätzen allgemein beschrieben. Diesen Reglungen ist nicht unmittelbar zu entnehmen, ob die Erfassung des Migrationshintergrundes in diesem Sinne für die Aufgabenerfüllung der Gesundheitsämter erforderlich ist. Es gibt hierzu lediglich eine Empfehlung einer Arbeitsgruppe innerhalb der Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden. Danach ist die Erfassung des Migrationshintergrundes bei der Einschulungsuntersuchung aus gesundheitspolitischer Sicht bedeutsam. Eine Rechtsgrundlage, aus der sich die Zulässigkeit der Verarbeitung dieser Daten ergibt, ist dies jedoch nicht. Der TLfDI hat dem TLVwA als Ergebnis seiner datenschutzrechtlichen Prüfung mitgeteilt, dass eine zusätzliche Erfassung des Migrationshintergrunds bei

den betroffenen Eltern nur dann zulässig ist, wenn die betreffenden Fragen auf dem Bogen eindeutig als freiwillig gekennzeichnet werden und die Eltern gemäß § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) auf den Zweck, den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung ihrer Daten sowie auf ihre Rechte auf Auskunftserteilung, Berichtigung und Löschung hingewiesen werden. Daraufhin erweiterte das TLVwA seine Anfrage dahingehend, ob der TLfDI grundsätzlich datenschutzrechtliche Bedenken gegen eine Erfassung des Migrationshintergrunds im Rahmen der Vorsorgeuntersuchungen des öffentlichen Gesundheitsdienstes – gemeint sind die anderen Kindertagesstätten- und Schuluntersuchungen, die in Thüringen durchgeführt werden – und die Übermittlung entsprechend aggregierter Daten an die Landesbehörden hat. Der TLfDI verwies in seiner erneuten Antwort wiederum auf die Problematik, dass es, wie vom TLVwA dargestellt, wohl fachliche Gründe für eine Erfassung dieser Daten gebe, eine ausdrückliche Rechtsvorschrift die Verarbeitung und Nutzung dieser personenbezogenen Daten jedoch nicht erlaubt oder anordnet. Soweit die Verarbeitung und Nutzung dieser Daten im Sinne von § 4 Abs. 1 Satz 2 ThürDSG „zur Erfüllung anerkannter Zwecke erforderlich ist“, besteht nach der gegebenen Rechtslage in diesen Fällen ausschließlich die Möglichkeit, bei den Eltern Daten zum Migrationshintergrund auf freiwilliger Basis entsprechend der oben dargestellten Verfahrensweise zu erheben. Gegen eine Übermittlung dieser auf freiwilliger Basis erhobenen Daten in aggregierter Form, die dann nicht mehr personenbezogen sind, bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Wann der Zusatzfragebogen bei der Einschulungsuntersuchung eingeführt wird, ist dem TLfDI noch nicht bekannt.

Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Die Erforderlichkeit muss sich vorliegend aus den Regelungen der ThürSchulGespflVO ergeben. Da diese Verordnung die betroffenen Eltern weder zur Auskunft über ihren Migrationshintergrund verpflichtet oder die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist, sind die Eltern auf die Freiwilligkeit ihrer Angaben hinzuweisen.

11.26 Datenbohrung bei der Kassenzahnärztlichen Vereinigung Thüringen

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ihm die Kassenzahnärztliche Vereinigung Thüringen auf seine bereits vor geraumer Zeit gestellte Frage, wie lange (Vergangenheit und Zukunft) die Daten über die zahnärztlichen Leistungen gespeichert werden, keine Antwort erteilt habe.
Da eine Auskunftsverweigerung im Raum stand, wandte sich der TLfDI an die Kassenzahnärztliche Vereinigung und bat unter Darlegung der Rechtslage um Mitteilung, weshalb denn der Beschwerdeführer keine Antwort erhielte. Der Auskunftsanspruch des Beschwerdeführers richtete sich nach § 83 Abs. 1 Sozialgesetzbuch (SGB) Zehntes Buch (X). Danach ist dem Betroffenen auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten bezieht, über die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und über den Zweck der Speicherung. Die Dauer der Speicherung ist zwar im Gesetz nicht genannt. Durch die Art der Auskunft muss der Betroffene jedoch in die Lage versetzt werden, zumindest in groben Zügen den Verwendungszusammenhang seiner Sozialdaten nachzuvollziehen und dessen Bedeutung bewerten zu können. Hierzu gehört nach Auffassung des TLfDI auch die Speicherdauer.
Die Kassenzahnärztliche Vereinigung teilte dem TLfDI mit, nach ihrem Dafürhalten habe sie dem Beschwerdeführer vollumfänglich die möglichen Auskünfte erteilt. Nachdem nämlich erst zu klären war, auf welcher konkreten Rechtsgrundlage der Beschwerdeführer Auskünfte verlangte (§ 83 SGB X oder § 305 SGB V), sei man zu dem Schluss gekommen, dass ein über die erteilte Auskunft hinausgehendes Informationsinteresse des Beschwerdeführers nicht zu erkennen und auch nicht über § 83 SGB X als Anspruchsgrundlage gedeckt sei. Die Fragestellung nach den Aufbewahrungszeiten von vertragszahnärztlichen Leistungen sei so allgemein gehalten, dass dem Erfordernis der genauen Bezeichnung seitens des Beschwerdeführers nicht nachgekommen worden sei. Hinsichtlich der Speicherung der Daten in der Vergangenheit und Zukunft sei die Anfrage zu unkonkret, sodass hierauf keine Auskunft gegeben werden konnte.

Im Übrigen könne nicht verbindlich beantwortet werden, wie lange in der Zukunft etwas gespeichert werde.
Das überzeugte den TLfDI nicht. Er teilte der kassenzahnärztlichen Vereinigung mit, dass er nach wie vor die Dauer der Speicherung der Daten über kassenzahnärztliche Leistungen vom Auskunftsrecht nach § 83 Abs. 1 SGB X umfasst ansehe. Da die Speicherdauer von zahnärztlichen Leistungen festzulegen bzw. gesetzlich festgelegt ist, war nicht nachvollziehbar, weshalb dies denn dem Beschwerdeführer nicht mitgeteilt werden könne. Daraufhin gab die Kassenzahnärztliche Vereinigung ihre Position auf und teilte dem Beschwerdeführer mit, dass sie zur Erfüllung ihrer Aufgaben Abrechnungsdaten zu zahnärztlichen Leistungen sechs Jahre verarbeitungsfähig vorhalte. Darüber hinaus würden bis zur Dauer von zehn Jahren komprimierte Daten zum Zweck der Datensicherung vorgehalten, um entsprechende Auswertungen für die Versorgungssituation in Thüringen vornehmen zu können. Hierbei werde jedoch eine Zuordnung von Daten zu Personen nicht mehr vorgenommen.
Der Beschwerdeführer bedankte sich, dass er letztendlich durch die Intervention des TLfDI zu der begehrten Auskunft über die Speicherdauer kam.

Eine Auskunft nach § 83 SGB X umfasst die zu einer Person gespeicherten Sozialdaten, deren Herkunft und die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, sowie den Zweck der Speicherung. Damit der Betroffene in die Lage versetzt wird, zumindest in groben Zügen den Verwendungszusammenhang seiner Sozialdaten nachzuvollziehen und dessen Bedeutung bewerten zu können, umfasst die Auskunft auch die Speicherdauer.

11.27 Auch zukünftig nur anonyme Daten für die Bundesärztestatistik

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde informiert, dass die Landesärztekammern zukünftig personenbezogene Daten von Ärzten als Einzeldatensätze an die Bundesärztekammer liefern sollen. Dies wäre ein Bruch mit der gegenwärtigen Praxis, bei der Arztdaten nur in aggregierter Form an die Bundesärztekammer fließen und somit kein Bezug zur Einzelperson hergestellt werden kann. Um hier Klärung im Interesse der vielen Thüringer Ärztinnen und Ärzte zu schaffen, die

ja Betroffene nach § 3 Abs. 1 Thüringer Datenschutzgesetz sind, bat der TLfDI die Thüringer Landesärztekammer um Stellungnahme. Dabei vertrat der TLfDI die Rechtsauffassung, dass für eine Weitergabe von personenbezogenen Daten an die Bundesärztekammer keine Rechtsgrundlage bestehe und somit eine Einwilligung des Betroffenen erforderlich wäre. Die Thüringer Landesärztekammer antwortete prompt und stellte klar, dass sie an der bisherigen Verfahrensweise festhalten wolle. Die Rechtsauffassung des TLfDI werde vollumfänglich geteilt. Somit war klar, dass die personenbeziehbaren Daten der Thüringer Ärztinnen und Ärzte auch in Zukunft die Landesärztekammer nicht verlassen müssen, jedenfalls nicht, wenn hierfür keine Rechtgrundlage besteht oder der Betroffene nicht wirksam eingewilligt hat.

Für statistische Zwecke sind anonymisierte Personendaten hinreichend. Eine Anonymisierung von Arztdaten, die von der Thüringer Landesärztekammer an die Bundesärztekammer geliefert werden, bleibt auch zukünftig gewährleistet. Der TLfDI konnte dies im Interesse der Thüringer Ärzteschaft klären und hat die Datenschutzbehörden des Bundes und der Länder über die Position der Landesärztekammer informiert.

11.28 Vertretung des Amtsarztes durch Private – die Zweite

Mit dem Thema der Vertretung des Amtsarztes durch private Ärzte beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 9. Tätigkeitsbericht (dort unter 11.5.). Damals wurde aufgrund einer Eingabe festgestellt, dass in einem Gesundheitsamt die schulzahnärztlichen Reihenuntersuchungen nicht nur von den Schulzahnärzten des Gesundheitsamts, sondern auch von privaten Zahnärzten durchgeführt wurden. Begründet worden war dies damit, dass die regulär beschäftigten Zahnärzte mehrwöchig arbeitsunfähig gewesen waren und die zahnärztliche Aufgabenerfüllung mit den angestellten Zahnärzten des Fachdienstes Gesundheit nicht mehr möglich gewesen war.
Dies begegnete nach Ansicht des TLfDI erheblichen datenschutzrechtlichen Bedenken. Nach § 55 Abs. 3 des Thüringer Schulgesetzes (ThürSchulG) sind die Schüler verpflichtet, sich den Maßnahmen des schulärztlichen und schulzahnärztlichen Dienstes zu unterziehen.

Bei einer Untersuchung durch den „Schul(zahn)arzt“ werden die Schüler nicht nur körperlich untersucht, es werden auch Gesundheitsdaten von ihnen erhoben. Eine zwangsweise Datenerhebung stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Dieser ist nur zulässig, wenn hierfür eine gesetzliche Grundlage besteht. Diese Grundlage ist in § 55 Abs. 3 ThürSchulG sowie in der nach § 55 Abs. 3 Satz 2 ThürSchulG erlassenen Rechtsverordnung zu sehen. Da § 1 Abs. 1 Satz 2 der Thüringer Verordnung über die Schulgesundheitspflege vorsieht, dass die Schulgesundheitspflege von den Schulärzten und Schulzahnärzten der Gesundheitsämter (schulärztlicher und schulzahnärztlicher Dienst) wahrgenommen wird, entspricht die Wahrnehmung dieser Aufgabe durch Private nicht den gesetzlichen Vorgaben. Vielmehr stellt die Schulgesundheitspflege eine hoheitliche Aufgabe dar, die nur durch einen Träger öffentlicher Gewalt wahrgenommen werden darf. Der TLfDI hatte dem damaligen Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) als oberste Aufsichtsbehörde seine Rechtsauffassung dargelegt und gebeten, die Gesundheitsämter in einem entsprechenden Rundschreiben über die Rechtslage aufzuklären. Außerdem sollte mitgeteilt werden, in welchen Gesundheitsämtern in Thüringen ebenfalls private Ärzte mit Aufgaben des schulärztlichen und schulzahnärztlichen Dienstes betraut sind.

Es stellte sich heraus, dass es an einigen Gesundheitsämtern in Thüringen üblich ist, Honorarärzte im schulärztlichen und schulzahnärztlichen Dienst zu beschäftigen. Grund dafür ist oftmals eine längere Krankheit oder Elternzeit des fest angestellten Arztes.

Der TLfDI hat gegenüber dem TMSFG mehrfach deutlich gemacht, dass eine derartige Situation nach seiner Rechtsauffassung mit der geltenden Rechtslage nicht vereinbar ist. Es wurde als unpraktikabel angesehen, im Vorfeld eine Einwilligung der Eltern zur Begutachtung des Kindes durch einen niedergelassenen Arzt einzuholen.

In dem Gesetzentwurf zur Änderung beamtenrechtlicher Vorschriften wurde das Problem aufgegriffen. § 33 Abs. 1 Thüringer Beamtengesetz regelt nun, dass angeordnete ärztliche Untersuchungen von den zuständigen Amtsärzten, beamteten Ärzten oder sonstigen von der zuständigen Stelle bestimmten Ärzten durchgeführt werden. Diese Bestimmung ist aber auf die Durchführung schulärztlicher Untersuchungen nicht direkt anwendbar, weil es sich hier nicht um angeordnete, sondern gesetzlich vorgesehene Untersuchungen han-

delt. So heißt es in der Gesetzesbegründung (Landtagsdrucksache 5/7453): „Absatz 1 regelt, welche Ärzte mit der Durchführung von Untersuchungen beauftragt werden dürfen. […] Die Möglichkeit zur Bestellung eines anderen ärztlichen Gutachters durch spezialgesetzliche Regelungen bleibt davon unberührt."
Der TLfDI verschließt sich nicht der Tatsache, dass im Einzelfall aufgrund von faktischen Problemen ein niedergelassener Arzt im schulärztlichen und schulzahnärztlichen Dienst einspringen muss. Diese Situation sollte aber die Ausnahme bleiben. Andernfalls muss es eine eindeutige gesetzliche Regelung geben, die zulässt, dass Aufgaben des schulärztlichen und schulzahnärztlichen Dienstes auch von anderen Ärzten durchgeführt werden können. Der TLfDI wird weiterhin mit dem nunmehr zuständigen Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie und den betroffen Gesundheitsämtern auf eine gesetzeskonforme Lösung hinarbeiten.

Da die verpflichtend durchzuführenden Schuluntersuchungen einen Grundrechtseingriff sowohl in das Grundrecht auf körperliche Unversehrtheit als auch in das Grundrecht auf informationelle Selbstbestimmung darstellen, dürfen sie nach geltender Rechtslage nur von Trägern hoheitlicher Gewalt durchgeführt werden.

11.29 Klinisches Krebsregister Thüringen

Die Überlebenschancen und die Lebensqualität krebskranker Menschen haben sich in den letzten Jahrzehnten in Deutschland erheblich verbessert. Allerdings steigen die Neuerkrankungsraten. Das Bundesministerium für Gesundheit hat gemeinsam mit der Deutschen Krebsgesellschaft, der Deutschen Krebshilfe und der Arbeitsgemeinschaft Deutscher Tumorzentren am 16. Juni 2008 den Nationalen Krebsplan initiiert. Ein Ziel des Nationalen Krebsplanes ist die Schaffung einer aussagekräftigen onkologischen Qualitätsberichterstattung für Leistungserbringer (wie z. B. Krankenhäuser und ambulant behandelnde Ärzte), Entscheidungsträger und Patienten durch einen flächendeckenden Ausbau der klinischen Krebsregister. Diese Aufgabe wurde mit dem Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und -registergesetz – KFRG) in Angriff genommen. Nach § 65c Sozialgesetzbuch (SGB) Fünftes Buch (V) erfolgt die Einrichtung klinischer Krebsregister durch die Län-

der, wobei die Daten flächendeckend und möglichst vollzählig erfasst sowie jährlich landesbezogen ausgewertet werden sollen. Die notwendigen rechtlichen Regelungen für die Einrichtung und den Betrieb klinischer Krebsregister einschließlich der datenschutzrechtlichen Bestimmungen bleiben den Ländern vorbehalten.

Das ursprünglich zuständige Thüringer Ministerium für Soziales, Familie und Gesundheit trat bereits frühzeitig an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran, um datenschutzrechtliche Fragen zur Umsetzung des KFRG abzustimmen. In Thüringen stellt sich, wie in den meisten neuen Bundesländern, die Situation etwas anders dar als in den meisten westlichen Bundesländern. Hier gab es bereits gewachsene Strukturen der klinischen Krebsregistrierung. In Thüringen existieren fünf regionale Klinische Krebsregister an den fünf Tumorzentren Erfurt, Gera, Jena, Nordhausen und Suhl. Diese Strukturen allein erfüllen aber nicht die Aufgaben, die § 65c SGB V dem künftigen Klinischen Krebsregister Thüringen zuweist. Zum einen muss eine nahezu flächendeckende Registrierung sichergestellt werden, es müssen Auswertungen der landesweit vorliegenden Daten möglich sein und die Daten der einzelnen vorhandenen Register müssen miteinander abgeglichen werden können, um Doppel- und Fehlmeldungen zu vermeiden.

Es wurden Verhandlungen darüber geführt, welche Rolle die fünf regionalen Klinischen Krebsregister bei der Erfüllung der gesetzlichen Aufgaben spielen werden und wie im Verhältnis dazu ein zentrales Register ausgestaltet werden soll. Es ist der Grundsatz der Datensparsamkeit zu beachten, es dürfen möglichst keine Daten doppelt vorgehalten werden. Gleichzeitig müssen die Zugriffsrechte der einzelnen Beteiligten wegen der Sensibilität der im Register gespeicherten Gesundheitsdaten sehr trennscharf geregelt werden. Der Prozess ist noch nicht abgeschlossen. Die Anforderungen des § 65c SGB V müssen bis zum 1. Januar 2016 erfüllt sein, allerdings gilt eine Übergangsregelung bis einschließlich 2017 (siehe § 65c Abs. 4 SGB V).

Auch das für die Umsetzung des KFRG in Thüringen notwendige Gesetzgebungsverfahren muss bis dahin abgeschlossen sein. Der TLfDI wird dieses im Hinblick auf die zu schaffenden datenschutzrechtlichen Regelungen begleiten und über das Ergebnis im nächsten Tätigkeitsbericht informieren.

Die klinischen Krebsregister sollen bundesweit flächendeckend ausgebaut werden. In Thüringen ist ein Klinisches Krebsregister Thüringen zu schaffen. Es ist der Grundsatz der Datensparsamkeit zu beachten. Die Zugriffsrechte der einzelnen Beteiligten müssen wegen der Sensibilität der im Register gespeicherten Gesundheitsdaten sehr trennscharf geregelt werden. Die notwendigen Datenübermittlungen bedürfen einer landesgesetzlichen Regelung.

11.30 Ist die Arztqualifikation auch echt?

Sie kennen das sicher: Beim Besuch in der Arztpraxis hängen häufig Urkunden und Fortbildungszertifikate zu Qualifikationen oder zusätzlichen Spezialisierungen und Lehrgängen. Dadurch wird dem Patienten angezeigt, welche Leistungen in der Praxis qualifiziert durch den Arzt oder durch das medizinische Fachpersonal durchgeführt werden können. Doch woher weiß der Patient, dass ein solches Fortbildungszertifikat auch echt ist?

Um dem Bürger die Möglichkeit zu geben, dies schnell und einfach prüfen zu können, betreibt die Landesärztekammer Thüringen mit anderen Ärztekammern ein Online-Portal bei der Bundesärztekammer https://www.kammerservice.de/, mit welchem die Prüfung dieser Urkunden möglich ist. Dafür ist auf der Urkunde ein QR-Code abgedruckt, der eine 64-stellige Zeichenfolge enthält. Diese Zeichenfolge ist die eindeutige Urkundennummer. Gibt man diese Zeichenfolge, welche man sich zuvor beim Arzt notiert oder etwa als Handyfoto gespeichert hat, in dem o. g. Portal ein, werden die Daten, welche auf der Urkunde abgedruckt sind, auch online angezeigt. So kann die Urkunde auf Echtheit überprüft werden.

Um diese Überprüfung technisch zu ermöglichen, werden hierzu die Daten von Urkunden und Fortbildungszertifikaten dezentral in den jeweiligen Landesärztekammern vorgehalten. Das Online-Portal, welches über die Bundesärztekammer betrieben wird, leitet die elektronischen Anfragen an die zuständigen Ärztekammern weiter. Anhand des Codes erkennt das Portal die zuständige Landesärztekammer.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte sich über die technische Si-

cherung der Zugänge, was insbesondere die Transportverschlüsselung vom Nutzer zum Portal-Server betraf. Außerdem wurde die Landesärztekammer Thüringen bezüglich der Bildungsvorschrift der Urkundennummer beraten. Hierbei war es vor allen Dingen wichtig, dass die Nummer, welche unter anderem aus dem Namen des Urkundeninhabers und weiteren Urkundendaten gebildet wird, nicht doppelt vorkommen darf, um die Eindeutigkeit der Urkunden zu gewährleisten. Hinsichtlich des Verfahrens in Thüringen steht der TLfDI mit der Landesärztekammer weiterhin in Kontakt, um die Sicherheit des Verfahrens abschließend beurteilen zu können. Das Verfahren selber befindet sich noch in der Testphase.

Wollen Bürger zukünftig die Echtheit einer Urkunde oder eines Fortbildungszertifikates vom Arzt- oder Medizinischem Fachpersonal prüfen, können sie diese über die Identifikationsnummer der Urkunde oder des Fortbildungszertifikates im Portal https://www.kammerservice.de/ kontrollieren. Wurde ein entsprechendes echtes Dokument gefunden, wird dieses zum Vergleich mit den wichtigsten Daten angezeigt. Der TLfDI prüft den Verifikationsdienst noch, um die Sicherheit abschließend beurteilen zu können.

11.31 Elektronische Gesundheitskarte: runde Sache oder Runder Tisch?

Seit dem 1. Januar 2015 gilt bundesweit ausschließlich die elektronische Gesundheitskarte als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkasse beim Arzt oder Zahnarzt. Hierauf wies der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in seiner Pressemitteilung vom 5. Januar 2015 hin (s. https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichu

ngen/pmtlfdi/150105_pm-e-gesundheitskarte.pdf). Für die Versicherten brachte die Einführung zunächst keine großen Änderungen mit sich, da auf der Karte lediglich die Daten abgebildet waren, die bislang auf der Krankenversichertenkarte enthalten waren, sowie zusätzlich das Geschlecht und ein Lichtbild des Versicherten. Diese Daten (außer dem Lichtbild) sind auch gemäß § 291 Abs. 2 Sozialgesetzbuch (SGB) Fünftes Buch (V) auf dem Chip der Krankenversicherungskarte gespeichert. Der geplante Onlineabgleich mit den gesetzlichen Krankenkassen sollte ab Mitte 2015 in verschiedenen Testregionen erprobt werden, zu denen Thüringen aber nicht zählte. Allerdings ist die elektronische Gesundheitskarte (siehe dazu Nr. 15.8.) darauf ausgerichtet, künftig zusätzliche Funktionen zu erfüllen, wie beispielsweise das so genannte E-Rezept und auf Wunsch des Patienten möglicherweise Notfallversorgungsdaten, elektronische Arztbriefe oder persönliche Arzneimittelrisiken und Unverträglichkeiten. Eine mögliche weitere Entwicklung ist zudem der Zugriff auf die elektronische Patientenakte. Der TLfDI hat der Landesärztekammer Thüringen und der Landesapothekerkammer Thüringen eine Gesprächsrunde angeboten, sofern dort Fragen oder Anregungen zur elektronischen Gesundheitskarte bestehen. Diese Stellen wollten bei Bedarf auf das Angebot zurückkommen.

Seit 29. Dezember 2015 ist das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze (sog. E-Health-Gesetz) in Kraft (siehe dazu Nr. 11.7.). Das Sozialgesetzbuch (SGB) Fünftes Buch (V) sieht bereits seit 2006 vor, dass auf der elektronischen Gesundheitskarte unter anderem Notfalldaten, elektronische Arztbriefe, Daten eines Medikationsplanes, eine elektronische Patientenakte und Erklärungen des Versicherten zur Organspenden gespeichert werden können, vgl. § 291a Abs. 3 SGB V. Damit allerdings all diese Funktionen der elektronischen Gesundheitskarte auch genutzt werden können, muss eine entsprechende Infrastruktur aufgebaut werden, die von allen Ärzten, Kliniken und Apotheken bundesweit einheitlich genutzt werden kann. Die verschiedenen Funktionen werden nun zehn Jahre nach Planung der Gesundheitskarte erst sukzessive zur Verfügung stehen. Das neue Gesetz stellt für verschiedene Funktionen in § 291b

SGB V einen Zeitplan bis zum 31. Dezember 2018 auf. Wer beruflich die Gesundheitskarte einsetzen muss, z. B. Ärzte, Kliniken und Apotheken, sollte sich daher gegebenenfalls vorab bei seinem Berufsverband informieren.
Das Gesprächsangebot des TLfDI an die Landesärztekammer Thüringen und die Landesapothekerkammer Thüringen, sofern es dort Fragen oder Anregungen zur elektronischen Gesundheitskarte gibt, steht daher nach wie vor.

Da auf der elektronischen Gesundheitskarte künftig Gesundheitsdaten der Patienten gespeichert werden sollen, müssen vor Ort die technischen und organisatorischen Maßnahmen getroffen werden, die zum Schutz dieser Daten erforderlich sind. Der TLfDI bietet den Berufsverbänden in Thüringen hierzu weiterhin seine Gesprächsbereitschaft an.

11.32 Betriebliches Eingliederungsmanagement, ein datenschutzrechtliches Minenfeld

Gemäß § 84 Abs. 2 Sozialgesetzbuch (SGB) Neuntes Buch (IX) ist der Dienstherr beziehungsweise die Dienststelle verpflichtet, betroffenen Beschäftigten, die länger als sechs Wochen krank sind oder waren, ein betriebliches Eingliederungsmanagement (BEM) anzubieten. Hierzu kann von der Personalverwaltung festgestellt werden, wie viele Krankheitstage als Voraussetzung vorliegen.
Zu der Frage, ob denn die Personalverwaltung befugt und berechtigt ist, auf der Grundlage einer Dienstvereinbarung zum BEM Mitteilungen zur Person und der Anzahl der Krankheitstage eines Beschäftigten an das in der Dienstvereinbarung vorgesehene Integrationsteam zu übermitteln, hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Folgendes ausgeführt:
Bei den Krankheitstagen von Beschäftigten handelt es sich um Personalaktendaten, für deren Verarbeitung oder Nutzung die dienstrechtlichen Vorschriften gelten, es sei denn, besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Einschlägige Vorschrift zur Vorlage von Personalaktendaten und Auskünften an Dritte ist § 85 Thüringer Beamtengesetz (ThürBG) in der seit 1. Januar 2015 geltenden Fassung. Eine Datenübermittlung zum Zweck der Durchführung eines BEM ist hier je-

doch nicht speziell geregelt, sodass die Zulässigkeit der Weitergabe/Datenübermittlung auf der Grundlage allgemeiner Vorschriften zu prüfen ist.
Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung personenbezogener Daten zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Datenschutzrechtlich streitig war in der Vergangenheit, ob und zu welchem Zeitpunkt der Personalrat über das Vorliegen der Voraussetzungen für die Durchführung eines BEM zu unterrichten ist. Nach der Rechtsprechung steht dem Personalrat die Möglichkeit zur Überprüfung zu, ob der Dienstherr seiner Verpflichtung zum Angebot eines BEM nachgekommen ist. Zu diesen Prüfzwecken kann unter Umständen auch verlangt werden, dass Namen von Betroffenen genannt werden.
Bezeichnend für das BEM ist, dass es nur auf Freiwilligkeitsbasis des Betroffenen und dessen Einwilligung durchgeführt werden kann und die betroffene Person bestimmt, welche Personen letztendlich damit befasst werden.
Die der Fragestellung zugrundeliegende abgeschlossene Dienstvereinbarung als sonstige Rechtsvorschrift schrieb die Weitergabe der Daten über krankheitsbedingte Fehlzeiten eines Betroffenen an das Integrationsteam vor, dem neben dem BEM-Beauftragten als Vertreter des Arbeitgebers ein Mitglied des Personalrats und gegebenenfalls der Schwerbehindertenvertretung angehören. Damit erhalten diese Personen bereits im Vorfeld, bevor es zu einer Willensäußerung des Betroffenen kommen kann, die Krankheitstage als Daten über das Vorliegen der Voraussetzungen zur Durchführung eines BEM. Willigt der Betroffene nicht ein, so sind dem Personenkreis personenbezogene Daten zu dem Betroffenen bekannt geworden, die letztendlich nicht zu einer weiteren Aufgabenerfüllung erforderlich sind. Die Übermittlung wäre daher nicht erforderlich und damit unzulässig.
Um dies zu vermeiden, sollten die Betroffenen von der Personalverwaltung selbst zum Zweck der Einholung einer Einwilligung zur Durchführung eines BEM angeschrieben werden. Damit würde vermieden, dass Personen, für die die personenbezogenen Daten eines Betroffenen mangels dessen Einwilligung für die weitere Aufgabenerfüllung nicht erforderlich sind, diese in unzulässiger Weise erhalten.

Die anfragende Stelle hat daraufhin die entsprechende Konkretisierung der Dienstvereinbarung zugesagt.

Da die Durchführung des Betrieblichen Eingliederungsmanagements von der Einwilligung des betroffenen Beschäftigten abhängt, bestimmt dieser letztendlich, wer außerhalb der Personalverwaltung seine personenbezogenen Daten über Krankheitstage verarbeiten darf. Es ist darauf zu achten, dass Personen, die mangels Einwilligung des Betroffenen letztendlich nicht mit der Durchführung des BEM befasst werden können, auch keine Informationen über die Krankheitstage erhalten.

11.33 Das Postgeheimnis gilt weiterhin! – Versendung von personenbezogenen Daten per Brief kein Datenschutzverstoß

Ein Rechtsanwalt beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Landesärztekammer Thüringen die IBAN und den BIC seines Mandanten mit der Post verschickt hatte. Hierin sah er einen Verstoß gegen das Thüringer Datenschutzgesetz (ThürDSG). Die Landesärztekammer Thüringen teilte auf Nachfrage des TLfDI mit, dass sie Beiträge für ihre Mitglieder erhebe. Hierzu können die Mitglieder der Landesärztekammer Einzugsermächtigungen erteilen. Dies sei auch durch den Mandanten des Beschwerdeführers geschehen. Die Landesärztekammer Thüringen stelle aus aktuellem Anlass das Lastschriftverfahren auf den SEPA-Zahlungsverkehr um und wollte ihrem Mitglied erneut die Möglichkeit anbieten, eine Einzugsermächtigung zu erteilen. Hierfür waren bereits die zutreffende IBAN und die BIC sowie das Kreditinstitut in dem übersandten Formular eingetragen. Dieses Formular war per Standardbrief zugesandt worden.
In der Versendung von personenbezogenen Daten mittels Brief durch die Post konnte der TLfDI keine Verletzung von § 9 Abs. 2 Nr. 1 ThürDSG erkennen. Aufgrund der zu treffenden technischen und organisatorischen Maßnahmen ist sicherzustellen, dass je nach Art der zu schützenden Daten gewährleistet ist, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können – Grundsatz der Vertraulichkeit. Die Vertraulichkeit von Postsendungen ist durch das Briefgeheimnis geschützt. Dieses wird von Artikel 10 des Grundge-

setzes garantiert. Das Postgesetz regelt, dass der Datenschutz bei Postdienstunternehmen nicht nur für Privatpersonen, sondern für alle Postkunden gilt. Weiterhin ist die Verletzung des Briefgeheimnisses nach § 202 Strafgesetzbuch (StGB) eine Straftat. Das Briefgeheimnis umfasst jedes Schriftstück, das verschlossen bzw. durch ein verschlossenes Behältnis gegen Kenntnisnahme gesondert gesichert ist. Damit liegt kein datenschutzrechtlicher Verstoß vor, wenn ein Dokument, das personenbezogene Daten des Empfängers enthält, mit der Post versandt wird. Diese Rechtsauffassung teilte der TLfDI sowohl der Landesärztekammer Thüringen als auch dem Beschwerdeführer mit.

Werden personenbezogenen Daten mit der Post in einem Standardbrief versandt, sind sie auf angemessene Weise vor dem Zugriff unberechtigter Dritter geschützt. Die Vertraulichkeit von Postsendungen ist durch das Briefgeheimnis geschützt, seine Verletzung ist nach § 202 StGB eine Straftat.

11.34 Auch Sozialbehörden dürfen nicht alles wissen

Ein Betreuer wandte sich im Namen des von ihm Betreuten an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Betreute erhielt Leistungen zur Rehabilitation und Teilhabe in Form von Eingliederungshilfen für behinderte Menschen. In dem zu ihm erstellten so genannten Gesamtplan war eine Fülle von Angaben enthalten, die der Betreuer für zu umfangreich hielt. Die im Gesamtplan erhobenen Daten dienen dem Sozialamt zur sozialhilferechtlichen und fachlichen Abklärung des individuellen Hilfebedarfs eines Bedürftigen nach Maßgabe von § 9 und § 53 ff. in Verbindung mit § 58 SGB XII. Ein Gesamtplan enthält Angaben zum Lebensbereich des Leistungsberechtigten. Auf dieser Grundlage können die Hilfeleistungen stetig an den Bedarf im Einzelfall angepasst und optimiert werden. Bei der Erstellung des Gesamtplans werden die am Hilfeprozess beteiligten Personen einbezogen.
Nach § 67a Abs. 1 SGB X dürfen Sozialdaten vom Sozialamt nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. An die Erforderlichkeit sind strenge Anforderungen zu stellen. Erforderlich ist die Kenntnis der Daten für das Sozialamt nur dann, wenn ohne diese Daten die Aufgabe nicht, nicht

vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Es genügt nicht, wenn eine Angabe zur Aufgabenerfüllung lediglich nützlich ist. Außerdem besteht nach § 67a Abs. 1 Satz 1 SGB X die gesetzliche Verpflichtung, Sozialdaten grundsätzlich beim Betroffenen zu erheben.

Die im Gesamtplan befindlichen Ausführungen zur Beschreibung der aktuellen Situation waren sehr ausführlich, teilweise durch Zitate des Betroffenen ergänzt und wurden an manchen Stellen nicht auf die Überschriften bezogen, unter denen sie sich fanden. Der Sozialhilfeträger wurde vom TLfDI gebeten, die Ausführungen im Gesamtplan nochmals auf die Erforderlichkeit für die Aufgabenerfüllung hin zu prüfen und den Gesamtplan gegebenenfalls zu überarbeiten. Dieses Unterfangen hat zunächst dazu geführt, dass neben kleineren Streichungen der Gesamtplan vom Sozialhilfeträger noch ergänzt und damit insgesamt erweitert worden ist. Hierzu wurde geltend gemacht, nur so könnten die Hilfeleistungen stetig angepasst und optimiert werden. Medizinische Daten beispielsweise dienten dabei als Grundlage für die Einschätzung des Leistungsanspruches und gäben Aufschluss über Defizite und Einschränkungen des Leistungsberechtigten.

Diese Auffassung teilt der TLfDI nicht umfänglich. Denn in den Gesamtplan gehören beispielsweise keine Mutmaßungen des sozialmedizinischen Dienstes hinsichtlich der vermeintlichen Ursachen eines Defizits im Verhalten des Betroffenen. In einem Gespräch mit dem Sozialamt konnte vermittelt werden, dass einige Feststellungen nicht notwendig waren und der Gesamtplan daher auf das erforderliche Maß reduziert werden muss. Ein endgültiges Ergebnis liegt noch nicht vor. Zumindest für die Zukunft ist aufgrund der Einführung der integrierten Teilhabeplanung (ITP), die der TLfDI begleitet hat (siehe dazu Nummer 16.1) davon auszugehen, dass die angesprochenen datenschutzrechtlichen Defizite zukünftig vermieden werden.

Ein ganz wichtiger Punkt ist auch, dass Antragsteller vor der Erstellung eines Hilfeplans regelmäßig schriftlich über alle Umstände informiert werden müssen, insbesondere auch darüber, welche Institutionen an der Beratung zum Hilfeplan in der so genannten Hilfeplankonferenz beteiligt werden. Sollte sich der Betroffene mit der namentlichen Behandlung seines Begehrens in der Hilfeplankonferenz nicht einverstanden erklären, müsste sein Anliegen in anonymer Form vorgestellt und beraten werden. Dieser Hinweis hat der Sozial-

hilfeträger aufgegriffen und die Erarbeitung eines entsprechenden Formulars zugesagt.

Auch bei der Erstellung eines Gesamtplans als Grundlage für Leistungen zur Rehabilitation und Teilhabe nach dem SGB IX dürfen personenbezogene Daten des Bedürftigen nur dann erhoben und verarbeitet werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Einer datenschutzrechtlichen Verbesserung zugeführt wurde die Aufklärung zur Einwilligung durch die Betroffenen.

11.35 Ein Jugendamt tat sich schwer, Auskunft zu erteilen

Mitunter ist die Bearbeitung einer Beschwerde sehr mühevoll. Bereits Mitte 2012 beschwerte sich ein Betroffener beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er vom Landratsamt keine Auskunft zu den über ihn bei einem Jugendamt verarbeiteten personenbezogenen Daten erhalten habe. Vom Jugendamt wollte er nämlich wissen, was eine Richterin beim Amtsgericht den Mitarbeiterinnen des Jugendamts mitgeteilt habe und was davon über ihn im Jugendamt gespeichert werde.
Auf Nachfrage des TLfDI teilte das Landratsamt mit, das Jugendamt sei für den Beschwerdeführer örtlich gar nicht zuständig. Nach einer Anhörung vor dem Familiengericht in einer Kindschaftssache, an dem eine Sachbearbeiterin des Jugendamts teilgenommen hatte, wurde das Landratsamt über einen „Auftritt“ des Beschwerdeführers bei der genannten Richterin per E-Mail informiert. Bis dahin sei der Beschwerdeführer im Landratsamt unbekannt gewesen. Seit diesem Vorfall gingen jedoch beim Landratsamt regelmäßig E-Mails des Beschwerdeführers ein, ohne dass das Landratsamt als Adressat erkennbar sei. Der Auskunftsanspruch des Betroffenen ging nach Auffassung des Landratsamts ins Leere, weil die E-Mail der Richterin gelöscht sei. Auf erneute Nachfrage des TLfDI übersandte das Landratsamt eine Sammlung von E-Mails des Beschwerdeführers und teilte mit, es halte an seiner Auffassung fest. Das Landratsamt verarbeite nämlich gar keine Daten des Betroffenen, es habe sich auch nicht zielgerichtet Daten des Beschwerdeführers beschafft, vielmehr habe der Beschwerdeführer seine personenbezogenen Daten aufgedrängt. Daher könne kein Anspruch des Beschwerdeführers

auf Auskunft nach § 13 Thüringer Datenschutzgesetz (ThürDSG) bestehen.
Nach Ausspruch einer Beanstandung nach § 39 ThürDSG wegen Verweigerung der Auskunft nach § 13 ThürDSG – obwohl keine der dort genannten Gründe vorlagen –, von der auch die Rechtsaufsicht benachrichtigt wurde, folgte ein weiterer umfangreicher Schriftwechsel. Letztendlich informierte die Rechtsaufsicht den TLfDI, das Landratsamt habe eine „Negativauskunft“ mit dem wesentlichen Inhalt erteilt, die E-Mail der Richterin sei vernichtet worden. Es existierten über den Beschwerdeführer dort keine wie auch immer gearteten Informationen, Daten, Unterlagen oder Akten. Zu seiner Person seien zu keinem Zeitpunkt Daten im Sinne des § 3 Abs. 3 ThürDSG verarbeitet worden.
Dies war so auch nicht ganz richtig. Tatsächlich sind selbstverständlich Daten zum Beschwerdeführer verarbeitet worden. Dies betraf zum einen die Löschung der E-Mail der Richterin, da eine Löschung nach der Definition des § 3 Abs. 3 Nr. 6 ThürDSG eine Datenverarbeitung darstellt. Zum anderen wurden personenbezogene Daten des Beschwerdeführers im Rahmen der Bearbeitung seiner Beschwerde zu seinem Auskunftsbegehren verarbeitet. Da aber die Löschung der E-Mail in der Auskunft genannt war und der TLfDI davon ausging, dass zum Jugendamt keine weiteren personenbezogenen Daten des Beschwerdeführers, insbesondere zur Beschwerdebearbeitung, gelangt sind, wurde der datenschutzrechtliche Verstoß als behoben angesehen.

Die Löschung personenbezogener Daten stellt eine Verarbeitung im Sinne des § 3 Abs. 3 Nr. 6 ThürDSG dar. Der Anspruch auf Auskunft nach § 13 ThürDSG geht ins Leere, wenn Daten gelöscht sind. Nach einer Löschung darf nicht mehr nachvollziehbar sein, um was für konkrete Daten es sich gehandelt hat. Im Rahmen der Bearbeitung eines Auskunftsersuchens werden ebenfalls personenbezogene Daten des Antragstellers verarbeitet. Die Auskunft, es seien keine Daten vorhanden, ist daher nicht richtig.

11.36 Aushang von Dienstplänen im Pflegeheim

Die Leitung eines Pflegeheims wandte sich Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil es datenschutzrechtliche Bedenken gegen

die Forderung der Heimaufsicht gab, die Dienstpläne der Pflegekräfte für alle Mitarbeiter und damit aufgrund der Gegebenheiten vor Ort auch für Heimbewohner zugänglich auszuhängen. Auf den zu verwendenden Dienstplänen war nämlich zu jedem einzelnen Mitarbeiter eine Vielzahl von Angaben für einen ganzen Monat vorgesehen: Name und Vorname der Pflegekraft, deren Qualifikation, wie viele Stunden und Urlaubstage aus dem Vormonat übertragen waren, wie viele Stunden sie nach dem Arbeitsvertrag zu arbeiten hat, wie viele Arbeitsstunden an welchem Tag geplant sind, an welchem Tag sie wegen Krankheit, eines kranken Kindes, Urlaubs aus verschiedensten Gründen oder wegen Mehrarbeit bzw. Überstunden frei hatte, sich im Mutterschutz oder in Kur, in der Schule oder auf einer Fortbildung befand und vieles mehr.
Mit dem Aushang wäre es nicht zu vermeiden gewesen, dass jeder Mitarbeiter der Pflegeeinrichtung, die Pflegeheimbewohner und deren Besucher diese persönlichen Daten der Beschäftigten zur Kenntnis nehmen konnten, wofür es keinerlei Rechtsgrundlage gab. Auf Nachfrage des TLfDI erklärte das Thüringer Landesverwaltungsamt als zuständige Heimaufsicht, es bestehe die grundsätzliche Erforderlichkeit, dass die Dienstpläne mit dem geschilderten Inhalt an personenbezogenen Daten der Mitarbeiter/innen angelegt würden. Die Pflegeheime seien verpflichtet, über den Einsatz der bei ihnen beschäftigten Mitarbeiter/innen einen Nachweis zu führen. Damit werde zum einen die Ausrichtung des Mitarbeitereinsatzes entsprechend den Regelungen aus dem Arbeitszeitgesetz, persönlicher, tariflicher oder betrieblicher Vereinbarungen und gegebenenfalls auch aus dem Bundesurlaubsgesetz belegt. Zum anderen werde mit dem Dienstplan die Einhaltung der vertraglichen Verpflichtung (Personaleinsatz laut Leistungs- sowie Vergütungsvereinbarung) nach dem Sozialgesetzbuch (SGB) Zehntes Buch (X) nachgewiesen. Auch bestehe für die Einrichtungsträger die Verpflichtung, den Einsatz der angestellten Mitarbeiter nach § 11 Abs. 1 Zif. 3 Thüringer Wohn- und Teilhabegesetz (ThürWTG) nachzuweisen. Bei aufsichtsrechtlichen Prüfungen in Pflegeeinrichtungen seien die Dienstpläne als wesentliches Qualitätskriterium erforderlich und dienten auch den diensthabenden Pflegekräften dazu, die Organisation der pflegerischen Versorgung sicherzustellen und Mitarbeiterausfälle zu kompensieren. Schließlich wurde vom Thüringer Landesverwaltungsamt ausgeführt, der Dienstplan sei rund um die Uhr für die anwesenden diensthabenden Pflegekräfte erforderlich, um die Organisation der

pflegerischen Versorgung sicherzustellen und Mitarbeiterausfälle kompensieren zu können.
Dass die einzelnen personenbezogenen Daten für unbefugte Dritte nicht einsehbar sein dürfen, war seitens der Heimaufsicht bisher noch nicht problematisiert worden. Der TLfDI hat dem Pflegeheim mitgeteilt, dass die Heimaufsichtsbehörde keinesfalls den Aushang der Dienstpläne mit den genannten Eintragungen zu den einzelnen Mitarbeitern für jedermann einsehbar fordern könne. Erforderlich und damit zulässig ist auch nach Auffassung der Heimaufsichtsbehörde lediglich, die Dienstpläne für aufsichtsrechtliche Kontrollen und intern den zuständigen diensthabenden Pflegekräften zur Sicherstellung der Organisation der pflegerischen Versorgung zur Verfügung zu stellen. Sofern die Dienstpläne nicht computergestützt geführt werden und damit keine technische Möglichkeit zur Verfügung steht, die Lesbarkeit personenbezogen zu beschränken, sind durch die zuständigen Heimleitungen oder Träger andere geeignete technische und organisatorische Maßnahmen zum Schutz der Mitarbeiterdaten vor unbefugter Kenntnisnahme zu treffen. Möglich ist es beispielsweise, gesonderte Dienstpläne zu erstellen und an für Pflegeheimbewohner und Besucher nicht zugänglichen Stellen auszuhängen, die nur die notwenigen Angaben der Anwesenheit enthalten.

Die Inhalte von Dienstplänen sind für aufsichtsrechtliche Prüfungen in Pflegeheimen erforderlich und dienen auch den diensthabenden Pflegekräften dazu, die pflegerische Versorgung sicherzustellen. Die Heimleitungen oder Träger haben entsprechende organisatorische und technische Maßnahmen zum Schutz vor unbefugter Kenntnisnahme der in den Dienstplänen enthaltenen Beschäftigtendaten durch andere Mitarbeiter oder Heimbewohner oder deren Besucher zu treffen. Mangels anderer Möglichkeiten ist der Datenumfang ausgehängter Dienstpläne auf das erforderliche Minimum zu reduzieren.

11.37 Sozialdatenübermittlung an die Staatsangehörigkeitsbehörden

In einem anderen Bundesland hatte sich ein Jobcenter an den zuständigen Landesbeauftragten für den Datenschutz gewandt und auf folgende Problematik hingewiesen:
Das dortige Jobcenter erhielt regelmäßig Anfragen von der im Innenministerium angesiedelten Staatsangehörigkeitsbehörde, um

festzustellen, ob ein Einbürgerungsbewerber, der die deutsche Staatsbürgerschaft erlangen möchte, die geforderten Voraussetzungen erfüllt. Hierzu gehört beispielsweise ein Nachweis, dass er sich in der Vergangenheit um eine Arbeitsstelle bemüht hat und von einer gewissen finanziellen Unabhängigkeit gegenüber dem Staat ausgegangen werden kann. Das zuständige Innenministerium wies darauf hin, dass in anderen Bundesländern hierzu eine mit den jeweiligen datenschutzrechtlichen Aufsichtsbehörden abgestimmte Einwilligungserklärung in die Datenübermittlung herangezogen werde. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) griff die zu dieser Problematik gestartete Länderumfrage auf und bat das (damalige) Thüringer Innenministerium (TIM) um Informationen zur Handhabung in Thüringen, da keine mit ihm abgestimmte Einwilligungserklärung bekannt war.

Das TIM teilte mit, es gäbe in Thüringen keine generelle Handlungsanweisung. Eine Anfrage an die Jobcenter im Rahmen des Einbürgerungsverfahrens erfolge nur in bestimmten Einzelfällen, wie bei wechselnden Arbeitsverhältnissen, Arbeitslosigkeit, geringen Einkommen und ähnlichen Fallkonstellationen. Für die Anfrage beim Jobcenter werde eine Einwilligung des Einbürgerungsbewerbers eingeholt, wofür ein Muster vorliege. Erteile ein Jobcenter die gewünschten Auskünfte nicht, müsse der Einbürgerungsbewerber aufgrund der allgemeinen Darlegungs- und Beweislast die benötigten Angaben selbst vorlegen. Also liege die Datenübermittlung daher vor allem auch im Interesse des Betroffenen und diene der Verfahrensvereinfachung. Die Vorgehensweise entspreche im Übrigen auch der Praxis in anderen Bundesländern und solle beibehalten werden.

Das übersandte Muster einer Einwilligungserklärung genügte aus Sicht des TLfDI jedoch nicht den Anforderungen an eine rechtswirksame Einwilligung. Vielmehr wurde mit der Unterschrift auf dem Formular eine pauschale Einwilligung erklärt, ohne dass der konkrete Zweck der Datenverarbeitung erkennbar war. Eine Einwilligung setzt aber nach § 4 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) voraus, dass diese in Bezug auf eine bestimmte Verarbeitung oder Nutzung der personenbezogenen Daten erklärt wird. Eine Übermittlung personenbezogener Daten von Seiten der aufgelisteten Behörden auf Grundlage des vorliegenden Musters war somit mangels rechtswirksamer Einwilligung unzulässig.

Zur Konkretisierung hätte daher zu den einzelnen Behörden, die auf dem Muster aufgelistet waren, jeweils eine Ergänzung hinzugefügt

werden müssen, welche konkreten Angaben des Betroffenen zu welchem konkreten Zweck eingeholt werden sollen. Rein praktisch bot es sich aus Gründen der Übersichtlichkeit nicht an, für die aufgelistete Vielzahl von Behörden aus unterschiedlichen Bereichen (Sicherheitsbehörden, Sozialbehörden etc.) dieselbe Mustereinwilligung zu nutzen.
Daraufhin hat das TIM die bis dahin genutzte Einwilligungserklärung zunächst in drei einzelne Erklärungen für Behörden, Sozialbehörden und Auslandsvertretungen des Herkunftsstaates aufgeteilt. Weiterhin war zu beachten, dass für verschiedene Behörden keine Einwilligungen erforderlich waren, weil die Beteiligung der Polizeibehörden, Strafverfolgungsbehörden, Gerichte, der Ausländer- und Ordnungsbehörden, der Auslandsvertretungen der Bundesrepublik, des Bundesamts für Migration und Flüchtlinge (BAMF), der Standesämter, Meldeämter und der Jugendämter auf Grundlage der gesetzlichen Regelungen der §§ 32 und 37 Abs. 2 Staatsangehörigkeitsgesetz (StAG) erfolgte.
Der TLfDI hielt es aber für angemessen, die Betroffenen auf die vielfältigen Anfragemöglichkeiten hinzuweisen, auch wenn dies nicht von ihrer Einwilligung abhing. Daher sollte die zunächst vorbereitete Einwilligung zu Abfragen bei den Meldebehörden, Ausländerbehörden, dem Bundesamt für Justiz, den Sicherheitsbehörden, dem Thüringer Landesamt für Verfassungsschutz, dem BAMF, dem Gewerbeamt, der Wohngeldstelle, dem Auswärtigen Amt und den deutschen Auslandsvertretungen als Merk- und Erläuterungsblatt umgearbeitet und genutzt werden. Dies dient der Transparenz für die Betroffenen, um ihnen die Möglichkeit zu geben, von den Datenübermittlungen Kenntnis zu erlangen.
Die Erhebung von Sozialdaten war nach § 67a Abs. 1 SGB X nur bei gesetzlich vorgesehener Einwilligung auf Einwilligungsbasis möglich. Entsprechend der Wertung nach § 67a Abs. 2 Nr. 1 SGB X war aber nach Auffassung des TLfDI dennoch die Erhebung auf Einwilligungsbasis möglich, um die Betroffenen vom Aufwand zu entlasten, sofern sie dies ausdrücklich wünschen.
Das TIM hat die Hinweise des TLfDI in den nunmehr zu verwendenden Einwilligungsmustern und insbesondere in einem ausführlichen Merkblatt für die betroffenen Einbürgerungswilligen berücksichtigt.

Ist zur Prüfung der Voraussetzungen in einem Verwaltungsverfahren eine Vielzahl von Bescheinigungen und Auskünften anderer Behörden erforderlich, können diese, sofern die gesetzlichen Voraussetzungen hierzu vorliegen, von der entscheidenden Behörde aufgrund von Einwilligungen der Betroffenen eingeholt werden. Besondere Bedeutung kommt hier der Transparenz für die Betroffenen zu.

11.38 Akteneinsicht beim Jugendamt – ein schwieriges Unterfangen?

Die Mutter eines volljährigen Sohnes, der zeitweilig in einem Heim untergebracht war, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ihr die Einsicht in die bzw. die Auskunft aus den beim Jugendamt zu ihrem Sohn geführten Akten verweigert würde. Ihr Akteneinsichts- bzw. Auskunftsrecht, das sie nach dem Bundesdatenschutzgesetz geltend machen wollte, hatte sie gegenüber dem Jugendamt „zum Zweck der Berichtigung und Löschung“ personenbezogener Daten beantragt. Das Jugendamt fragte nach, welche personenbezogenen Daten, die beauskunftet werden sollten, die Beschwerdeführerin als unrichtig ansehe. Trotz der umfangreichen Antwort der Beschwerdeführerin sah sich das Jugendamt immer noch nicht imstande, Akteneinsicht zu gewähren bzw. Auskunft zu erteilen. Dies interpretierte die Beschwerdeführerin als Ablehnung ihres Antrags und bat den TLfDI um Hilfe.

Der TLfDI nahm zur Sachverhaltsklärung Akteneinsicht im Jugendamt. Dabei wurde festgestellt, dass die eingesehenen, zum Sohn geführten Akten auch personenbezogene Daten der Beschwerdeführerin enthielten. Sie enthielten aber jeweils ebenso personenbezogene Daten Dritter, auch des Kindsvaters sowie der mit den einzelnen Sachverhalten beschäftigten Mitarbeiter des Jugendamts und des Heims. Die Akten waren darüber hinaus bereits abgeschlossen. Der Sohn war zwischenzeitlich volljährig, sodass für ihn auch keine weitere Zuständigkeit des Jugendamtes bestand. Es war eine zehnjährige Aufbewahrungsfrist festgelegt worden

Innerhalb eines konkreten Verwaltungsverfahrens beim Jugendamt besteht für die betroffenen Kinder, für die Eltern und Personensorgeberechtigten (gemeinsam oder allein) sowie die übrigen Beteiligten eines solchen Verfahrens ein Anspruch auf Akteneinsicht nach § 25 Zehntes Buch Sozialgesetzbuch (SGB X). Das Jugendamt hat

Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 25 Abs. 1 SGB X). Die Verpflichtung zur Gestattung der Akteneinsicht besteht nicht, soweit die Vorgänge wegen der berechtigten Interessen anderer Beteiligter oder dritter Personen geheim gehalten werden müssen (§ 25 Abs. 3 SGB X).
Da eine Trennung zwischen den personenbezogenen Daten der Beschwerdeführerin und Daten Dritter nicht möglich war, musste der Anspruch auf Akteneinsicht vom Jugendamt sorgfältig geprüft werden. Die Antragstellerin muss darlegen, welche Daten aus welchem Grund für die Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich sind. Außerdem muss das Jugendamt für die dann in Betracht kommenden Daten prüfen, ob sie wegen der berechtigten Interessen anderer Beteiligter oder dritter Personen geheim gehalten werden müssen. Bei Ablehnung der Akteneinsicht steht der Antragstellerin eine rechtsmittelfähige Entscheidung zu.
Der TLfDI hat daher das Jugendamt gebeten, die Antragstellerin aufzufordern, ihren Antrag dahingehend zu konkretisieren, welche Daten aus welchem Grund für die Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich sind.
Daneben hat das Jugendamt dem Betroffenen nach § 83 SGB X auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung.
Im Rahmen der Auskunftserteilung auf dieser Rechtsgrundlage kann es – wie im vorliegenden Fall – ausreichen, der Beschwerdeführerin mitzuteilen, welche Schreiben von ihr in der betroffenen Akte enthalten sind und welche Schreiben an sie gerichtet wurden.
Hierauf wies der TLfDI das Jugendamt hin, dass der Beschwerdeführerin nach der Konkretisierung ihres Antrags unter Berücksichtigung der Rechtsauffassung des TLfDI Auskunft erteilen wird.

Nach § 13 Thüringer Datenschutzgesetz haben Betroffene das Recht auf Auskunft und Akteneinsicht gegenüber den öffentlichen Stellen des Landes. Auskunftsrechte können sich auch auf spezialgesetzliche Rechtsgrundlagen wie §§ 25 Abs. 1 und 83 SGB X stützen. Ein Antrag auf Auskunft muss so hinreichend konkretisiert werden, dass

der auskunftspflichtigen Behörde eine Entscheidung über den Antrag möglich ist.

11.39 Wohngeld nur für gläserne Bürger?

Ein Betroffener, der Wohngeld beantragen wollte, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil von ihm nicht etwa nur Angaben zu seinen Einkünften, sondern auch eine detaillierte Aufstellung seiner durchschnittlichen monatlichen Ausgaben verlangt wurde. Verlangt wurden Angaben zu Ausgaben für die Ernährung (Frühstück, Mittag- und Abendessen), Neuanschaffung von Bekleidung, Reinigung und Reparatur von Schuhen, Kleidung und Wäsche, Haushaltsgegenständen und Möbeln, für die persönlichen Dinge des täglichen Lebens (einschließlich Kosmetik, Körperpflege, Bücher, Zeitschriften, Vereine, Hobby usw.) bis hin zu Telefon, Hörfunk, Fernsehen, Versicherungen und zu guter Letzt detaillierten Kosten für ein Kraftfahrzeug (Versicherung, Steuer, Treibstoff, Wartung, Reparatur). Am Ende des Merkblatts zum Wohngeldantrag wurde von der zuständigen Sozialbehörde auch gleich darüber informiert, dass unvollständige Angaben zur Ablehnung des Wohngeldantrags führen.
Mit den beschriebenen Angaben wäre der Antragsteller für die Sozialbehörde der gläserne Mensch schlechthin. Sein gesamter Lebenswandel wäre anhand seiner Ausgaben nachvollziehbar. Inwieweit derartige Angaben auf die Ermittlung der Höhe des Wohngelds Einfluss haben können, erschloss sich dem TLfDI nicht. Nach dem Wohngeldgesetz sind lediglich die Einkommensverhältnisse zu klären. Demnach ist eine Datenerhebung als unzulässig anzusehen, die über die im Wohngeldgesetz konkret geregelten Erhebungstatbestände hinausgeht. Der Nachweis monatlicher Ausgaben für den aufgeführten persönlichen Bedarf gehört keinesfalls dazu.
Die zur Stellungnahme aufgeforderte Stadtverwaltung teilte mit, Grundlage der Befragung bilde § 15 Wohngeldgesetz (WoGG). Nach der Allgemeinen Verwaltungsvorschrift zur Durchführung des Wohngeldgesetzes seien die Angaben der wohngeldberechtigten Personen besonders auf ihre Glaubhaftigkeit und Vollständigkeit zu überprüfen (Plausibilitätsprüfung), wenn sich bei der Ermittlung des Jahreseinkommens unter dem Bedarf liegende Einnahmen ergäben. Glaubhaft sei nur, wenn das angegebene, zur Verfügung stehende Einkommen plus Wohngeld 80 % des Bedarfs nach dem Sozialge-

setzbuch Zwölftes Buch (SGB XII) ergebe. Mit anderen Worten: Plausibel ist nur, wenn man mit Wohngeld über mehr als 80 % des Sozialhilfesatzes verfügt. Oder anders herum: Wer nicht genügend Einkommen hat oder angibt, kann davon nicht leben und schummelt vielleicht – soll so eine Person Wohngeld bekommen?
Aufgrund des Einschreitens des TLfDI hat das Sozialamt das Standardschreiben geändert. Der Vordruck zur Datenerhebung werde nur noch als Erleichterung und Hilfe für Wohngeldberechtigte angeboten. Die Betroffenen seien nicht verpflichtet, die Angaben zur durchschnittlichen persönlichen Verwendung der schmalen Einkünfte auszufüllen. Machen die Betroffenen aber keine Angaben, würde – soweit aufgrund der eingereichten Unterlagen möglich – das nicht plausibel dargelegte Einkommen geschätzt und die Regelsätze nach dem SGB II und SGB XII als persönlicher Bedarf angesetzt. Dies könne aber im Einzelfall dem Antragsteller dann zum Nachteil gereichen, wenn er die freiwilligen Angaben nicht vornehme.
Diese Maßnahme reichte dem TLfDI natürlich nicht aus. Die Erhebung von Sozialdaten ist nach § 67a SGB X nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe nach dem SGB erforderlich ist. Das Wohngeldgesetz gehört nach § 68 SGB I zum Sozialgesetzbuch und gibt genaue Vorgaben zur Ermittlung der Höhe des Wohngeldes. Das Wohngeld berechnet sich nach der Anzahl der zu berücksichtigenden Haushaltsmitglieder (§§ 5 bis 8 WoGG), der zu berücksichtigenden Miete oder Belastung (§§ 9 bis 12 WoGG) und dem Gesamteinkommen (§§ 13 bis 18 WoGG). Zu diesen Punkten darf die zuständige Stelle grundsätzlich personenbezogene Daten erheben. Welche Daten bei der Einkommensermittlung zugrunde zu legen sind, regeln die §§ 13ff.WoGG. Insoweit steht fest, welche konkreten Angaben hierfür erforderlich sind.
Wird Wohngeld beantragt, besteht für die Antragsteller eine sozialrechtliche Mitwirkungspflicht (§ 60 SGB I). Damit verbunden ist die Obliegenheit, der Wohngeldstelle Auskunft über die Einnahmen und über andere für das Wohngeld maßgebende Umstände zu geben. Demnach ist der Antragsteller verpflichtet, sein Einkommen offenzulegen, nicht jedoch Daten dazu, wie und für welche Dinge er sein Einkommen im Einzelfall ausgibt. Es ist unzulässig, vom Antragsteller Informationen zu verlangen, die weder Einnahmen noch für das Wohngeld maßgebende Umstände betreffen. Also war es völlig unerheblich, welche Beträge speziell für Ernährung, für persönliche Dinge des täglichen Lebens und die Neuanschaffung von Bekleidung

aufgewandt werden. Weshalb diese Angaben eine Plausibilität begründen sollten, war nicht nachvollziehbar. Also forderte der TLfDI das Sozialamt auf, das Formular nicht mehr zu verwenden.
Im Sinne der Bürgerfreundlichkeit entwarf das Sozialamt nun ein neues Schreiben für die Wohngeldempfänger und verlangte immer noch freiwillig Angaben zur Lebensführung, weil diese doch für die Betroffenen günstig seien. Gleichzeitig wurden die Betroffenen aber auf mögliche ungünstige Rechtsfolgen bei Verweigerung der Angaben hingewiesen. Aber auch dies war nicht zu akzeptieren.
Der Hinweis für die Betroffenen auf die Freiwilligkeit der zu ergänzenden Angaben zum Wohngeldantrag am Ende des Vordrucks war nicht hilfreich. Die Freiwilligkeit der Angaben musste klar und deutlich erkennbar sein. Es war nicht davon auszugehen, dass Betroffene zuerst den ganzen Vordruck lesen und sich dann entscheiden, ob sie ihn ausfüllen oder von ihrem Recht Gebrauch machen, die Angaben nicht zu machen. Daher sollte bereits unmittelbar nach der Überschrift hervorgehoben vorangestellt werden, dass die folgenden Angaben freiwillig sind (vgl. § 67a Abs. 3 Satz 2 SGB X). Dabei war auch deutlich darauf einzugehen, dass – wie vom Sozialamt vorgetragen – die Gewährung von Rechtsvorteilen im Vordergrund steht, die Angaben ggf. aber auch im gesetzlichen Rahmen zu Ungunsten ausfallen können.
In einem Gespräch legte das Sozialamt nochmals dar, die beabsichtigte Datenerhebung solle zu dem Zweck erfolgen, dem Antragsteller die richtige Hilfe angedeihen zu lassen. Wenn das angegebene Einkommen deutlich unter dem festgestellten Regeleinkommen liege, spreche viel dafür, dass er entweder Hilfe zum Lebensunterhalt oder Leistungen nach dem SGB II beziehen könne. Dagegen war aus datenschutzrechtlicher Sicht einzuwenden, dass, selbst wenn jemand einen Anspruch nach SGB II hat, dies einem Anspruch auf Wohngeldzahlung nur entgegensteht, wenn er diese Leistung nach SGB II auch empfängt. Es reicht eben nicht immer aus, wenn eine Behörde davon ausgeht, eine Datenerhebung erfolge doch nur im Interesse des Betroffenen. Der TLfDI wies nochmals darauf hin, dass das SGB keinen Raum für die Datenerhebung auf Grundlage einer Einwilligung bietet, es sei denn, das Gesetz sieht dies ausdrücklich vor. Dies ist jedoch im Zusammenhang mit der Beantragung von Wohngeld nicht gegeben. Daher verbleibt es bei dem Grundsatz, dass die Erhebung von Sozialdaten nach § 67a Abs. 1 Satz 1 SGB X nur zulässig

ist, wenn ihre Kenntnis zur Aufgabenerfüllung nach diesem Gesetzbuch erforderlich ist.
Nach den gesetzlichen Vorschriften muss ein Antragsteller bei der Beantragung von Wohngeld nur sein Einkommen nachweisen, jedoch nicht, wofür er dieses verwendet. Auch die vorgetragenen Beweggründe für die Datenerhebung zur Plausibilitätsprüfung änderten daran nichts.
Im Ergebnis hat das Sozialamt mitgeteilt, der streitige Vordruck werde nicht mehr verwandt. In Fällen, in denen ein großes Missverhältnis der angegebenen Einkünfte zu den Bedarfsätzen nach dem SGB II und SGB XII besteht, wird der Betroffene zukünftig angehört. Er kann dann darlegen, wie er es schafft, „über die Runden zu kommen“ und wird auf die Möglichkeit des Erhalts weiterer Leistungen hingewiesen. Hiergegen ist aus datenschutzrechtlicher Sicht nichts einzuwenden.

Die Einwilligung von Betroffenen kann im Sozialrecht nur dann eingeholt werden, wenn die sozialrechtlichen Vorschriften eine Einwilligung ausdrücklich zulassen. Im Rahmen des Antrags auf Wohngeld können nur Einkommensnachweise verlangt werden.

11.40 Datenerhebung zur Aufnahme von Klienten anderer Sozialhilfeträger

Ein privater Träger, der betreute Wohngruppen und betreutes Einzelwohnen für Abhängigkeitserkrankte anbot, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er datenschutzrechtliche Bedenken zu der Anforderung des Sozialamtes hatte. Dieses wollte mit einem Formblatt zur Datenerhebung Informationen zu Bewohnern erhalten, die aus anderen Kommunen stammten.
Auf Nachfrage des TLfDI teilte das Sozialamt mit, dass die Datenerhebung zur Abstimmung der Aufnahme von Klienten anderer Sozialhilfeträger im Rahmen des ambulant betreuten Wohnens für Leistungsberechtigte nach §§ 53 ff. Sozialgesetzbuch (SGB) Zwölftes Buch (XII) dienen sollte. Damit war vom Wohnheimträger anzugeben, wer der zuständige Sozialhilfeträger eines betroffenen, allerdings nicht namentlich zu nennenden Klienten war und ob bzw. welche Hilfen nach dem SGB XII und anderen Bestimmungen bereits erbracht wurden. Darüber hinaus sollte die Notwendigkeit der

Aufnahme des Klienten außerhalb des Zuständigkeitsbereichs des bisherigen Sozialhilfeträgers begründet und der erwartete Hilfebedarf eingefügt werden. Die Problematik bestand darin, dass die geforderten Angaben nicht vom konkret betroffenen Klienten (Grundsatz der Erhebung beim Betroffenen) oder von der bisher für diesen zuständigen Stelle (dem anderen Sozialträger), sondern von der aufnehmenden Einrichtung angegeben werden sollte. Fraglich war auch, ob der Wohnheimträger denn über die Angaben überhaupt verfügte oder diese erst vom Betroffenen erheben musste.
Das Sozialamt legte zur Erläuterung dar, es ginge darum, erst einmal die Bedarfe der „eigenen“ Bürger der Kommune zu decken und festzustellen, inwieweit eine „Eigennutzung“ der vorhandenen Platzkapazität bestehe. Unter dem Blickwinkel des Datenschutzes habe man den Fragebogen bewusst anonym gehalten. Die Praxis habe gezeigt, dass Sozialhilfeträger oder andere zuständige Stellen bei entsprechenden Leistungserbringern vor Ort Kapazitätsanfragen stellten, die meist gekoppelt sind mit Fragen zu konzeptionellen Inhalten, speziellen Ausrichtungen usw. Um die Kapazitätsanfrage in Höhe der gegebenenfalls benötigten Fachleistungsstunden konkret abklären zu können, würden die im Fragebogen enthaltenen Daten benötigt.
Der Fragebogen enthielt keine Namen der Betroffenen und war damit zunächst anonym. Soweit Angaben verlangt wurden und hierzu jeweils ein Stichwort genügte, war die Anonymität nicht aufgehoben.
Der TLfDI hat darauf hingewiesen, dass bei den Angaben zur Begründung der Notwendigkeit der Aufnahme des Klienten außerhalb des Zuständigkeitsbereichs des bisherigen Sozialhilfeträgers darauf zu achten ist, dass keine Angaben gemacht werden, die eine Reanonymisierung des Betroffenen ermöglichen. Um dies sicherzustellen, wurde das Sozialamt gebeten, die Träger auf diese Gefahr hinzuweisen.
Damit bestanden keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Vorgehensweise des Sozialamtes.

Eine Erhebung von Angaben über Dritte ist datenschutzrechtlich unbedenklich, wenn die Anonymität des Betroffenen gewahrt wird, die Daten bei der zur Auskunft berufenen Stelle vorhanden und zur Aufgabenerfüllung der Auskunftsbegehrenden Stelle erforderlich sind.

11.41 Datenschutz und Sorgerechtsstreitigkeiten

Ein Vater (Beschwerdeführer) beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über das Jugendamt eines Landkreises zum Umgang mit seinen personenbezogenen Daten in einer Gerichtsverhandlung. In dem Verfahren ging es um das Sorgerecht für seinen Sohn. Nach der Meinung des Beschwerdeführers hatte nämlich das Jugendamt in der Gerichtsverhandlung von ihm allerdings nicht näher bezeichnete unwahre Angaben über ihn verlautbart. Außerdem vertrat er die Auffassung, das Jugendamt unterliege der Amtsverschwiegenheit und hätte daher nur mit seiner Einwilligung bei Gericht Angaben machen dürfen. Im Übrigen hatte er das Jugendamt unter Fristsetzung aufgefordert, ihm Auskunft zu den über ihn gespeicherten personenbezogenen Daten zu erteilen. Dem sei das Jugendamt nicht nachgekommen.

Der TLfDI wies den Beschwerdeführer zunächst darauf hin, dass dem Jugendamt als Beteiligtem im gerichtlichen Verfahren zum Sorge- und Umgangsrecht mit Kindern eine maßgebliche Rolle zukommt und eine Verpflichtung der Mitarbeiter besteht, auf Fragen des Gerichts Auskünfte zu erteilen. Zu beachten ist, dass es in dem gerichtlichen Verfahren zuvorderst um das Wohl des Kindes geht. Die Rolle des Jugendamts wird nicht von den anderen Prozessbeteiligten bestimmt. Angaben bei Gericht sind somit regelmäßig auch nicht von einer Einwilligung eines anderen Prozessbeteiligten abhängig, und es bedarf hierzu grundsätzlich auch keiner Schweigepflichtentbindung. Daraufhin wollte es der Beschwerdeführer, ohne dass er den Sachverhalt konkret schilderte, genau wissen und verlangte vom TLfDI die Angabe sämtlicher Rechtsgrundlagen, aufgrund derer ein Jugendamt Daten übermitteln darf. Dem nachzukommen hielt der TLfDI weder für zielführend noch für angezeigt, ohne dass eine Stellungnahme des Jugendamts in der Angelegenheit vorlag.

Das Landratsamt teilte dem TLfDI mit, das Jugendamt habe aufgrund seiner Mitwirkungspflicht nach § 50 Sozialgesetzbuch (SGB) – Achtes Buch (VIII) das Familiengericht bei allen Maßnahmen, die die Sorge von Kindern und Jugendlichen betreffen, zu unterstützen und sei daher Verfahrensbeteiligter im streitgegenständlichen Verfahren gewesen. In dieser Eigenschaft sei in der nichtöffentlichen Sitzung beim Amtsgericht von einer Mitarbeiterin mündlich Bericht

erstattet worden. Alles, was über den Beschwerdeführer in diesem Zusammenhang an Informationen aufgenommen worden sei, befände sich in der Gerichtsakte. Weitere Daten zu dem Beschwerdeführer seien beim Landratsamt nicht gespeichert. Dem Beschwerdeführer habe das Landratsamt zwischenzeitlich eine entsprechende Auskunft gegeben.
Datenschutzrechtliche Bedenken bestanden zu der vom Landratsamt dargelegten Vorgehensweise nicht.

Ist ein Jugendamt Beteiligter in einem gerichtlichen Verfahren, ist es verpflichtet, in Wahrnehmung seiner gesetzlichen Aufgaben die erforderlichen Angaben zu machen. Datenschutzrechtliche Gründe stehen dem nicht entgegen. Zulässige Angaben bei Gericht sind nicht von der Einwilligung eines anderen Prozessbeteiligten abhängig.

11.42 Sozialhilfe auf falschem Konto: Datenschutz leitet auf richtiges Konto um

Der Betreuer einer in einem Pflegeheim untergebrachten älteren Dame beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er war der Auffassung, dass der behördliche Beauftragte für den Datenschutz eines Landratsamts (bDSB) zu lax mit seiner Beschwerde umgegangen sei und den Datenschutz bei der Bearbeitung verletzt habe. Der Betreuer schilderte, er habe für die Betreute bei dem zuständigen Landratsamt Sozialhilfe zur Überweisung auf deren Konto beantragt. Die nach seiner Auffassung falsch berechnete Sozialhilfe sei dann aber einschließlich des Taschengelds für die Betreute nicht auf ihr Konto, sondern auf das Konto des Pflegeheimbetreibers überwiesen worden. Das Taschengeld habe der Betreiber des Pflegeheims letztendlich erst auf Intervention des Sozialamts auf das Konto der Betreuten überwiesen.
Gegen den Sozialhilfebescheid hatte der Betreuer Widerspruch eingelegt und diesen gesondert auch an den bDSB versandt, weil er darin auch die Verletzung datenschutzrechtlicher Vorschriften geltend gemacht hatte. Der bDSB hatte hierauf nicht reagiert, was der Betreuer nicht hinnehmen wollte.
Der TLfDI hat dem Betreuer zunächst erläutert, dass er in seiner gesetzlichen Funktion als Kontrollbehörde für öffentliche Stellen keine Weisungsbefugnis gegenüber den nach § 10a Thüringer Daten-

schutzgesetz (ThürDSG) bei den Daten verarbeitenden Stellen bestellten bDSB hat. Der TLfDI konnte daher den bDSB in Person nicht, wie vom Betreuer gewünscht, auffordern, eine Antwort auf den Widerspruch gegen den Sozialhilfebescheid zu geben. Der bDSB ist in seiner Funktion dem Leiter der Daten verarbeitenden Stelle (hier Landratsamt) unmittelbar zu unterstellen und hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken.
Für den TLfDI ist die Arbeitsweise eines Beauftragten für den Datenschutz vor Ort nur beschränkt überprüfbar. Beispielsweise kann die notwendige Fachkenntnis zu den Fragen des Datenschutzes und der Datensicherheit hinterfragt und geprüft werden oder ob seine Tätigkeit keinem unüberwindbaren Interessenskonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt ist. Ansonsten ist für Einhaltung der datenschutzrechtlichen Vorschriften bei der Verarbeitung der personenbezogenen Daten die öffentliche Stelle verantwortlich, und sie unterliegt der Kontrolle des TLfDI nach § 37 ThürDSG.
Der Umgang mit der Beschwerde wegen der Überweisung der Sozialhilfe auf das Konto des Pflegeheims seitens des Landratsamts war also vom TLfDI nach § 11 ThürDSG zu prüfen und zu bewerten. Der TLfDI hat daher das Landratsamt zur Stellungnahme aufgefordert. Mangels einer konkreten Rechtsgrundlage konnte die Überweisung der Sozialhilfe auf das Konto des Pflegeheimbetreibers nämlich nur auf Verlangen des Hilfeempfängers oder mit dessen Einwilligung erfolgen. Das Landratsamt teilte mit, man habe die Angelegenheit geprüft und festgestellt, dass die Überweisung der Sozialhilfe leider ohne die erforderliche Einwilligung der Berechtigten auf das Konto des Pflegeheims erfolgte. Es sei die übliche Verfahrensweise, die direkte Zahlung der Sozialhilfe an das Pflegeheim zu leisten. Zur grundsätzlichen Entlastung der Hilfeempfänger und der Betreuer werde dies in der Regel sehr gerne in Anspruch genommen. In zukünftigen Fällen werde jedoch in Absprache mit dem bDSB sichergestellt, dass ohne die erforderliche Einwilligung des Betroffenen keine Zahlungen unmittelbar an das Pflegeheim bzw. dessen Träger erfolgen. Damit wird zukünftig den datenschutzrechtlichen Erfordernissen Rechnung getragen.

Das Handeln eines bDSB ist der öffentlichen Stelle zuzuschreiben, die der Kontrolle des TLfDI unterliegt. Sozialhilfe darf nicht einfach

ohne Verlangen oder Einwilligung des Betroffenen auf das Konto des Pflegeheims überwiesen werden, auch wenn dies in der Regel gerne von den Hilfeempfängern in Anspruch genommen wird. Der Fall zeigt wieder einmal, dass, auch wenn etwas im Sinne der Betroffenen gut gemeint ist, dies nicht immer auch in seinem Interesse sein muss.

11.43 Illegaler Datenhandel auch bei Thüringer Behörden? – Zur Anwerbung von neuen Krankenversicherten

Gegen Ende des Jahres 2013 informierte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz über ein Verfahren gegen ein Versicherungsunternehmen wegen des Verdachts des illegalen Datenhandels. Das Versicherungsunternehmen hatte ein bundesweites Netz von Vertrauensleuten aufgebaut, aus dem heraus Hinweise auf mögliche Kunden, insbesondere junge Beamtinnen und Beamte, gegeben werden. Diesem Vertrauensleutesystem gehörten zum erheblichen Teil auch Mitarbeiter des öffentlichen Dienstes an. In der überregionalen Presse war die Rede von mehr als 10.000 Beamten. Insofern war es angeraten, die Landesregierungen auf die Ermittlungen anzusprechen und anzuregen, dass insbesondere bei den personalverwaltenden Stellen des Landes und der Kommunen untersucht wird, in welchem Umfang Mitarbeiter des öffentlichen Dienstes als Vertrauensleute des Versicherungsunternehmens fungierten, wie diese Nebentätigkeit praktisch ausgestaltet war, ob sie angezeigt und vergütet war.
Beschäftigten- und Bewerberdaten im öffentlichen Dienst unterfallen dem Personalaktengeheimnis. Ihre Weitergabe ist an die gesetzlichen Regelungen gebunden. Für die Weitergabe durch Mitarbeiter von Personalverwaltungen an ein Versicherungsunternehmen existiert grundsätzlich keine Befugnis.
Weiteren Pressemeldungen zufolge hatten im Zuge der Bestechungsvorwürfe gegen Mitarbeiter des Versicherungsunternehmens auch Durchsuchungen der Geschäftsstellen in Thüringen stattgefunden. Weiterhin wurde bekannt, dass die Anklagebehörde seit geraumer Zeit gegen unbekannte Mitarbeiter auch der öffentlichen Verwaltung ermittle. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat diese Entwicklung zum Anlass genommen, die Landesregierung auf die Problematik aufmerksam zu machen. Die Nutzung und Weitergabe von perso-

nenbezogenen Daten von Beschäftigten und Bewerbern, die dem Personaldatenschutz unterfallen, würden einen Verstoß gegen datenschutzrechtliche Vorschriften darstellen. Gemäß dem damals gültigen § 93 Abs. 2 und dem seit 1. Januar 2015 gültigen § 85 Abs. 2 Thüringer Beamtengesetz (ThürBG) dürfen Auskünfte an Dritte nur mit Einwilligung des Betroffenen gegeben werden, sofern die dort formulierten Ausnahmen nicht vorliegen. Durch den Verweis auf die dienstrechtlichen Vorschriften in § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gilt dies ebenso für Tarifbeschäftigte. Für die Vermittlungstätigkeit für eine Versicherung gelten keine Ausnahmen von dem Einwilligungserfordernis. Daher regte der TLfDI an, insbesondere die personalverwaltenden Stellen des Landes und der Kommunen auf die Problematik hinzuweisen. Rückinformationen zu tatsächlichen Feststellungen, dass Beschäftigte in personalverwaltenden Stellen unbefugt Personaldaten von dort Beschäftigten übermittelt hätten, gab es nicht.
Das Bußgeldverfahren hatte der LfDI Rheinland-Pfalz Ende des Jahres 2014 einvernehmlich mit dem Versicherungsunternehmen abgeschlossen. Grundlage hierfür war unter anderem die Umstellung des Vertriebs bei dem Versicherungsunternehmen. Die Datenschutzbestimmungen sollen zukünftig insbesondere auch dadurch eingehalten werden, dass neue Kundenwerbungen durch Informationen von Kollegen oder Kontaktaufnahmen ohne das Einverständnis der Betroffenen für die Zukunft ausgeschlossen werden.
Konkrete Hinweise darauf, dass personalverwaltende Stellen in den öffentlichen Stellen des Freistaats Thüringen an dem illegalen Datenhandel beteiligt gewesen sein könnten, sind dem TLfDI nicht zur Kenntnis gelangt.
Der TLfDI nimmt auch hier sachdienliche Hinweise gern entgegen.

Personaldaten unterliegen einem besonderen Schutz. Die Übermittlung von Daten eines Beschäftigten im öffentlichen Dienst an ein Versicherungsunternehmen zum Zweck der Kundenwerbung ist nur mit Einwilligung des Betroffenen zulässig.

11.44 Das Jugendamt hat alles richtig gemacht

Eine Mutter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie habe sich mehrmals in einer Unterhaltssache an das Jugendamt einer Stadt mit

der Bitte um Akteneinsicht gewandt und keine Antwort erhalten. Außerdem habe das Jugendamt die in der Unterhaltssache beteiligte Gegenpartei, den Vater des unterhaltsberechtigten Kindes, angerufen und unaufgefordert über die Inhalte des Schreibens der Bürgerin an das Jugendamt informiert.
Der TLfDI schrieb das Jugendamt mit der Bitte um Stellungnahme an. Nach § 25 Abs.1 Sozialgesetzbuch (SGB) Zehntes Buch (X) muss die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt.
Das Jugendamt teilte mit, dass die Beschwerdeführerin persönlich im Jugendamt vorgesprochen habe. Dort seien ihr die Entscheidungen zur Unterhaltsberechnung im konkreten Fall erläutert worden. Die von ihr schriftlich gestellten Fragen seien beantwortet worden. Ihr seien die vom Kindsvater nachgereichten Unterlagen vorgelegt und von Akteninhalten Kopien überlassen worden. Der Vorwurf, dass keine Akteneinsicht gewährt worden sei, wurde deshalb vom Jugendamt zurückgewiesen. Zur telefonischen Kontaktierung des Kindesvaters teilte das Jugendamt mit, dass der Kindesvater nach dem letzten Schreiben der Beschwerdeführerin telefonisch informiert worden sei, dass die Kindesmutter weitere Fragen zur Unterhaltsberechnung habe. Des Weiteren seien mit dem Kindesvater die noch offenen Fragen besprochen worden. Er wurde durch das Jugendamt aufgefordert, weitere Unterlagen nachzureichen und im Jugendamt vorzusprechen.
Der TLfDI hat keine Anhaltspunkte dafür gefunden, dass die schriftlichen Erläuterungen des Jugendamtes nicht den Tatsachen entsprachen. Eine unzulässige Übermittlung von Sozialdaten an den Kindesvater erfolgte nach dieser Darlegung nicht. Es gab keine Anhaltspunkte dafür, dass die schriftlichen Erläuterungen des Jugendamtes nicht den Tatsachen entsprachen. Sie waren alle mit konkreten Terminen und weiteren Einzelheiten belegt worden. Dies wurde der Beschwerdeführerin mitgeteilt. Der Aufforderung des TLfDI, sich hierzu nochmals zu äußern, kam sie nicht nach. Daher bestand kein weiterer Handlungsbedarf.

Die Behörde muss den Beteiligten Einsicht in die das Verfahren betreffenden Akten gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. In welcher Weise dies geschieht, ist nicht verbindlich festgelegt. Es reicht gegebenenfalls auch eine mündliche Information und die Übergabe von Kopien aus der Akte.

11.45 Sozialdatenschutz im Eilverfahren

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil eine Stadt Sozialdaten bei Dritten erhoben hatte. Dem lag folgender Sachverhalt zugrunde:
Der Betroffene hatte die Stadt in einem Eilverfahren verklagt, ihm die Kosten der Unterkunft zuzusichern und seine Umzugskosten zu übernehmen. Es handelte sich dabei um den „klassischen" Ausnahmefall der Vorwegnahme der Hauptsache. Sofern eine positive Entscheidung für den Antragsteller im einstweiligen Verfahren getroffen worden wäre, wäre diese später in einem folgenden Hauptsacheverfahren nicht mehr revidierbar gewesen. Nach dem Eingang der Antragsschrift bei der Stadt betrug die Frist zur Stellungnahme eine Woche. Da der Umzugstermin kurz danach anberaumt worden war, musste die Stadt damit rechnen, dass unmittelbar nach der Antragserwiderung durch die Stadt auch eine gerichtliche Entscheidung folgen würde.
Kurzfristig wurde eine Vorortbesichtigung der neuen Wohnung vom Außendienst der Stadt veranlasst. Es wurde festgestellt, dass das Klingelschild bereits mit dem Namen des Beschwerdeführers sowie mit dem Namen einer weiteren Person beschriftet worden war. Da der andere Name aus der Verwaltungsakte nicht bekannt war, lag die Vermutung nicht fern, dass eine weitere Person mit in der Wohnung lebte, was sich auf die Höhe des Anspruchs nach dem Sozialgesetzbuch (SGB) Zweites Buch (II) ausgewirkt hätte. Die Stadt nahm an, dass eine Nachfrage und direkte Erhebung beim Betroffenen angesichts der anwaltlichen Vertretung nur über den Prozessbevollmächtigten hätte erfolgen können, was innerhalb der Frist zur Stellungnahme nicht mehr aussichtsreich erschien. Sie nahm daher Kontakt mit dem Vermieter auf, um in Erfahrung zu bringen, welche Personen die Wohnung bewohnten. Damit hatte die Stadt Jena Sozialdaten bei einem Dritten erhoben.

Letztendlich kommt es bei der datenschutzrechtlichen Bewertung darauf an, ob der betreffende Mitarbeiter der Stadtverwaltung nach § 67a Abs. 2 Nr. 2 Buchstabe b, bb) SGB Zehntes Buch (X) Sozialdaten bei dem Vermieter hätte erheben dürfen. Dies wäre der Fall, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert hätte und keine Anhaltspunkte dafür bestanden hätten, dass seine überwiegenden schutzwürdigen Interessen beeinträchtigt würden. Schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten sprechen, sind insbesondere dann gegeben, wenn der Leistungsträger notwendigerweise Sozialdaten des Betroffenen an den Dritten übermitteln muss, um die Datenerhebung zu ermöglichen. So kann auch die direkte Kontaktaufnahme, die damit verbunden ist, dass der Vermieter erfährt, dass eine Person Leistungsempfänger nach dem SGB II ist, Anhaltspunkt für eine Beeinträchtigung seiner schutzwürdigen Interessen sein.
Die Stadt berief sich auf den konkreten Missbrauchsverdacht, weswegen das schutzwürdige Interesse des Betroffenen zurücktreten müsse. In seinem Urteil vom 25. Januar 2102 (Az.: B 14 AS 65/11R) legte das Bundessozialgericht dar, dass schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten im Rahmen des § 67a Abs. 2 Nr. 2 Buchst. b, bb SGB X sprechen könnten, wegen einer hohen Eilbedürftigkeit der Angelegenheit zurückgestellt werden.
Allerdings hat die Stadt den Wortlaut des § 13 Abs. 3 SGB X nicht vollständig beachtet. Danach muss sich die Sozialbehörde zwar an den Bevollmächtigten wenden, der für das Verfahren bestellt ist. Sie kann sich aber auch an den Beteiligten selbst wenden, soweit er zur Mitwirkung verpflichtet ist. Wendet sich die Behörde an den Beteiligten, muss der Bevollmächtigte verständigt werden. Nach all dem wäre wohl auch eine Erhebung beim Betroffenen möglich gewesen. Angesichts der hohen Eilbedürftigkeit war es aber nicht rechtsfehlerhaft, in der konkreten Situation vom Vorliegen der Voraussetzungen des § 67a Abs. 2 Nr. 2 Buchstabe b, bb SGB X auszugehen.
Die Stadt hat mitgeteilt, dass der vorliegende Sachverhalt deutlich vor Augen geführt habe, dass sich – auch und gerade in Eilsituationen – die Grenzen der zulässigen Datenerhebung in einem Bereich abspielen, der juristisch nur schwer erfassbar ist. Das hier im Streit stehende Verfahren war für die Stadt Anlass, die mit der gerichtlichen Vertretung befassten Mitarbeiter nochmals im Umgang mit Sozialdaten zu sensibilisieren und darauf hinzuwirken, dass in jedem

Einzelfall die Interessen des Betroffenen sorgsam in den Blick zu nehmen sind, bevor sich für ein Abweichen vom Grundsatz der unmittelbaren Datenerhebung entschieden wird.

Sozialdaten dürfen nur in den engen gesetzlich benannten Ausnahmefällen bei Dritten erhoben werden. Schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten sprechen, sind insbesondere dann gegeben, wenn der Leistungsträger notwendigerweise Sozialdaten des Betroffenen an den Dritten übermitteln muss, um die Datenerhebung zu ermöglichen. Im Einzelfall kann eine hohe Eilbedürftigkeit für die Zulässigkeit der Datenerhebung bei Dritten sprechen.

11.46 Anonymisierung von Pflegedienstmitarbeitern zum Zweck der Entgeltsatzverhandlungen

Regelmäßig müssen Pflegeheimträger und Pflegedienste im Rahmen der mit dem hierfür zuständigen überörtlichen Sozialhilfeträger (Thüringer Landesverwaltungsamt – TLVwA) geführten Entgeltsatzverhandlungen auf der Grundlage des Sozialgesetzbuchs (SGB) Zwölftes Buch (XII) auch anonymisierte Daten zu den eingesetzten Mitarbeitern vorlegen.
Eine Rehabilitationseinrichtung hatte sich anwaltlich vertreten an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt, mit dem Vorbringen, das TLVwA verlange zur Plausibilisierung der prospektiv zu vereinbarenden Entgeltsätze Einsicht in die Personalakten sämtlicher der für die Einrichtung tätigen Beschäftigten – rückwirkend seit 2012. Darüber hinaus sollten ebenfalls zur Plausibilisierung der nach §§ 75 ff. SGB XII zu verhandelnden Entgeltsätze – nach Personalnummern geordnet – Aufstellungen sämtlicher Beschäftigter über deren Bruttovergütung, die gesetzlichen Gehaltsabzüge, die Nettovergütung sowie Eingruppierung vorgelegt werden.
Der TLfDI schrieb das TLVwA an und vertrat die Auffassung, da es sich bei Personalakten um eine Sammlung personenbezogener Daten über die jeweils Betroffenen handele, sei zu differenzieren, ob die Einsicht in alle Unterlagen erforderlich ist oder ob sich die Kenntnis auf konkret zu bezeichnende Angaben eingrenzen lässt. Unter Umständen reiche die Auskunft zu diesen Angaben aus oder die Einsicht lasse sich auf einzelne Dokumente beschränken. Auf diese Weise

werde eine Verarbeitung personenbezogener Daten vermieden, die in den Unterlagen vorhanden, für die Aufgabenerfüllung der öffentlichen Stelle jedoch nicht erforderlich seien.
Das TLVwA bestritt, Personalakten verlangt zu haben. Ein entsprechendes Verlangen konnte aus dem vorgelegten Schriftwechsel nicht entnommen und daher nicht bewiesen werden. Weiterhin teilte das TLVwA dem TLfDI mit, dass aus der aktuellen Rechtsprechung heraus eine plausible und nachvollziehbare Darlegung der prospektiven „Gestehungskosten“ für die Prüfung vorausgesetzt werde. Die tatsächlichen Personalkosten seien anzuerkennen, wenn sie sich aus der vorliegenden Tarifbindung bei funktionsgerechter Eingruppierung ergeben. Der Träger habe hierzu eine Nachweispflicht. Bislang seien von der Einrichtung die Stellennummern mit Angabe von Funktionsbereich, Eingruppierung und wöchentlicher Arbeitszeit vorgelegt worden, die im Zusammenhang mit dem für den Träger gültigen Tarifwerk eine vorläufige Prüfung zugelassen haben. Es müsse jedoch zusätzlich überprüft werden, ob mit jeder Stellennummer auch eine tatsächliche Stellenbesetzung verbunden sei. Die Stellennummer resultiere nämlich im vorliegenden Fall ausschließlich aus dem Soll-Stellenplan heraus und umfasse auch möglichweise nicht besetzte Stellen. Deshalb müssten die Personalnummern genannt werden, weil diese den Schluss auf die tatsächliche Besetzung eindeutig zuließen. Dies gehe im Übrigen mit dem Urteil des BSG vom 29. Januar 2009 (B3P7/08R) konform, da bei Zweifeln über die voraussichtlich künftigen Gestehungskosten die Nachweispflicht der Einrichtung bis zum Nachweis der in der Vergangenheit angefallenen Kosten reicht. Eine namentliche Untersetzung der Personalnummer werde nicht verlangt, da dies tatsächlich dem in der Rechtsprechung und in der Schutznorm des § 85 Abs. 3 Satz 5 SGB XI vorgegebenen Grundsatz widersprechen würde, wonach personenbezogene Daten zu anonymisieren sind.
Der TLfDI teilte der Rehabilitationseinrichtung seine datenschutzrechtliche Bewertung unter Einbeziehung des Vorbringens des TLVwA mit. Danach sind Personalnummern unter der Voraussetzung, dass eine konkrete namentliche Mitarbeiterliste vorliegt, personenbeziehbar. Werden nur die Personalnummern ohne Bezüge zu den natürlichen Personen angegeben, kann von einer anonymisierten Darstellung ausgegangen werden. Eine Anonymisierung liegt dann vor, wenn keine oder nur mit unverhältnismäßigem Aufwand mögliche Zuordnung zu den Namen der betroffenen Beschäftigten besteht

(§ 85 Abs. 3 Satz 5 SGB XII).Daher konnten die Angaben der Personalnummern zur weiteren Prüfung der tatsächlich besetzen Stellen vom TLVwA angefordert werden.
Kurze Zeit später meldete sich die Vertretung anderer Einrichtungen und beklagte sich darüber, dass das TLVwA sich mit der bisherigen Praxis der Angabe von Stellennummern oder Kürzeln der einzelnen Mitarbeitern nicht mehr zufriedengebe und ab sofort unter Berufung auf das Schreiben des TLfDI nun die Personalnummern der Mitarbeiter verlange. Sie bat daher den TLfDI um verbindliche Mitteilung, unter welchen Umständen die Benennung von Personalnummern unter den datenschutzrechtlichen Gesichtspunkten zulässig ist und/oder wie anderweitig rechtlich verfahren werden kann, um schützenswerte Belange der Mitarbeiter in ihren Mitgliedseinrichtungen nicht zu verletzen.
Der TLfDI hat hierzu erläutert, dem zitierten Schreiben habe ein zu prüfender Sachverhalt zugrunde gelegen, in dem das TLVwA einen erhöhten Prüfaufwand geltend machte, nachdem es Zweifel an den Angaben einer antragstellenden Einrichtung gab. Unter diesem Blickwinkel wurde die Angabe der Personalnummer als zulässig erachtet. Dies schließe jedoch nicht aus, dass auch Kürzel von Mitarbeitern eine datenschutzgerechte Lösung darstellen können. Der TLfDI hatte in der Bearbeitung der ersten Anfrage auf den dargelegten Sachverhalt abgestellt, jedoch kein allgemeingültiges Erfordernis postuliert. Aus datenschutzrechtlicher Sicht sind daher beide Benennungsmöglichkeiten in der Liste aus Gründen der Unterscheidbarkeit akzeptabel.

Sind nach den Vorschriften des Sozialgesetzbuchs anonymisierte Daten von Beschäftigten zu Prüfungszwecken vorzulegen, muss sichergestellt sein, dass keine oder nur mit unverhältnismäßigem Aufwand eine Zuordnung zu den einzelnen Beschäftigten möglich ist. Soweit die Unterscheidbarkeit der einzelnen Beschäftigten aus Plausibilitätsgründen zu Prüfzwecken erforderlich ist, kann dem nachgekommen werden, indem die Kürzel der Mitarbeiter oder deren Personalnummer oder deren Stellenzeichen angegeben werden. Entscheidend ist, dass der Prüfbehörde grundsätzlich keine Reanonymisierung möglich sein darf.

11.47 Medizinische Diagnose in Behördenbescheid – kein Problem

Ein Bürger wandte sich mit folgendem Anliegen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI): Er hatte von einem Landratsamt einen Bescheid erhalten, in dem sein Antrag auf die Erteilung eines Schwerbehindertenausweises nach § 69 Abs. 5 Sozialgesetzbuch (SGB) Zehntes Buch (X) mit der Begründung abgelehnt worden war, dass festgestellt worden sei, der Betroffene leide an dem Asperger-Syndrom und habe infolgedessen nur leichte soziale Anpassungsschwierigkeiten. In der Benennung der konkreten ärztlichen Diagnose neben den festgestellten Beeinträchtigungen sah der Betroffene einen Datenschutzverstoß.
Diese Auffassung konnte der TLfDI nicht bestätigen. Die Behörde durfte die personenbezogenen Daten das Beschwerdeführers verarbeiten, da aufgrund seines Antrags die Datenverarbeitung zum Aufgabenbereich der Behörde gehört, § 67c SGB X. Für den ablehnenden Bescheid gelten die formalen Anforderungen nach § 33 ff. SGB X. Es handelt sich um einen Verwaltungsakt, der inhaltlich hinreichend bestimmt sein muss, § 33 Abs. 1 SGB X. Er ist außerdem mit einer Begründung zu versehen, § 35 Abs. 1 Satz 1 SGB X. Nach Auffassung des TLfDI waren die Ausführungen zu medizinischen Diagnosen erforderlich, um die von der Behörde getroffene Entscheidung näher zu begründen. Der Bescheid ist an den Betroffenen gerichtet und geht damit auch nur ihm per Post zu. Sofern der Bescheid bei anderen Stellen vorlegt werden muss, kann gegebenenfalls eine Kopie angefertigt werden, in der die Schwärzung medizinischer Angaben möglich ist. Daher bestanden gegen die Aufnahme der Diagnosen in dem konkreten Bescheid keine datenschutzrechtlichen Bedenken.

Wenn der Bescheid einer Behörde an einen Betroffenen gerichtet wird, muss in diesem Bescheid alles stehen, was zur Begründung der Entscheidung erforderlich ist. Das gilt auch, wenn es sich um sensible Angaben wie Gesundheits- oder Sozialdaten handelt.

11.48 Wohin mit dem Schriftverkehr zum Betrieblichen Eingliederungsmanagement (BEM)?

Niemand ist absolut sicher vor Erkrankung: Erkältung, Grippewelle, Rückenprobleme und weitere Beeinträchtigungen führen zur Arbeitsunfähigkeit. Wenn Beschäftigte jedoch innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, hat der Gesetzgeber ein Hilfsangebot vorgesehen. Nach § 84 Abs. 2 Sozialgesetzbuch (SGB) Neuntes Buch (IX) wird der Arbeitgeber mit Zustimmung und Beteiligung der betroffenen Person verpflichtet, mit der zuständigen Interessensvertretung zu klären, wie die Arbeitsunfähigkeit möglichst überwunden und mit welchen Leistungen und Hilfen erneuter Arbeitsunfähigkeit vorgebeugt werden kann. Ziel des so genannten betrieblichen Eingliederungsmanagements (BEM) ist es, den Arbeitsplatz zu erhalten. Die betroffene Person/der Bedienstete kann der Durchführung eines BEM zustimmen oder dies ablehnen.

Dem Angebot an einen Betroffenen zu einem BEM-Gespräch kommt besondere Bedeutung zu, weil die Dienststelle dem Personalrat aufgrund dessen Kontrollfunktion unter Umständen beweisen können muss, dass sie ihrer Verpflichtung nach § 84 Abs. 2 SGB IX nachgekommen ist.

Ein Betroffener fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach, ob es denn in Ordnung sei, dass seine Antwort auf das Angebot, egal, ob er es annehme oder nicht, zur Personalakte genommen werde.

Nach § 50 Beamtenstatusgesetz gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden (§ 81 Abs. 1 Satz 1 Thüringer Beamtengesetz – ThürBG). Das Angebot zu einem BEM-Gespräch kann aus Sicht des TLfDI als im unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehend angesehen werden und ist daher konsequenterweise in der Personalakte abzuheften. Die Abheftung in der Personalakte hat den Vorteil, dass damit der Schutz für besonders sensible personenbezogene Daten automatisch hergestellt ist.

Von der Personalakte zu unterscheiden sind andere Akten (Sachakten), in denen auch Schriftstücke mit personenbezogenen Daten Beschäftigter abgelegt werden können, die für das Dienstverhältnis

verarbeitet oder genutzt werden. Da sich im Falle der Ablehnung eines BEM-Gesprächs keine weiteren Konsequenzen für den Betroffenen oder sein Dienstverhältnis ergeben und das Anschreiben an den Betroffenen wie oben ausgeführt nur dem Nachweis des Angebots nach § 84 Abs. 2 SGB IX dient, hat es der TLfDI in der Vergangenheit nicht kritisiert, wenn das Angebot der Dienststelle mit der Ablehnung zu einer hierzu angelegten Sachakte genommen wurde. Dem Betroffenen stehen hierzu ebenfalls Einsichtsrechte zu (§ 84 Abs. 4 ThürBG), sodass für ihn keine Nachteile erkennbar sind. Für den Vorgang sind entsprechende Aufbewahrungsfristen vorzusehen.

Zum Nachweis, dass dem Betroffenen ein Angebot zum Eingliederungsmanagement nach § 84 Abs. 2 SGB IX unterbreitet wurde, kann der Schriftverkehr zur Personalakte genommen werden. Es bestehen aber auch keine durchgreifenden datenschutzrechtlichen Bedenken, die Angebote mit den ablehnenden Antworten von Betroffenen in einer hierzu geführten Sachakte abzuheften.

11.49 Löschungsresistente Daten im Gesundheitsamt

Im Rahmen seiner Kontrolltätigkeit ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass der KJÄD (= Kinder- und Jugendärztlicher Dienst) der Gesundheitsämter in Thüringen im Rahmen von Einschulungsuntersuchungen ein Programm verwendet, bei dessen Benutzung datenschutzrechtliche Probleme bei der Datenlöschung bestehen. Zum einen erfolgt in diesem System keine automatische Löschung der hochsensiblen Patientendaten, sondern nur eine Archivierung zum Stichtag des 18. Geburtstags, wobei aber der Zugriff auf diese Daten wohl über diesen Zeitpunkt hinaus weiterhin möglich ist. Zum anderen ist der Zugriff auf eine so genannte Zentralkartei offensichtlich von allen Arbeitsplätzen aus uneingeschränkt möglich. Das bedeutet, dass Mitarbeiter des KJÄD auch auf Patientendaten zugreifen können, die sie zu ihrer Aufgabenerfüllung eigentlich nicht (mehr) benötigen. Die Gesundheitsämter in Thüringen wurden vor diesem Hintergrund vom TLfDI angeschrieben und gefragt, ob das betreffende Programm im Rahmen von Einschulungsuntersuchungen seitens des KJÄD angewandt wird und wenn ja, inwieweit die Möglichkeit für den Dienst besteht, die Zugriffsrechte der Benutzer auf die für sie notwendigen Informationen zu

beschränken. Es wurde auch gebeten mitzuteilen, ob der KJÄD ein Rollen- und Berechtigungskonzept für die Zugriffsrechte erstellt hat oder andere Beschränkungsmöglichkeiten bestehen. Die Gesundheitsämter wurden gebeten darzulegen, ob dort entsprechende Vorkehrungen nach § 9 Thüringer Datenschutzgesetz getroffen wurden oder schriftliche Regelungen zur regelmäßigen Löschung von Patientendaten bestehen. Nach Auffassung des TLfDI muss die Löschung manuell, etwa durch einen Mitarbeiter, erfolgen, sofern es keine Möglichkeit einer automatischen Löschung der nicht mehr benötigten Daten gibt.
Aus den Antworten der Gesundheitsämter ließ sich entnehmen, dass alle Gesundheitsämter sehr bemüht sind, datenschutzrechtliche Vorgaben einzuhalten. Dort ist man sich der Notwendigkeit des sorgsamen Umgangs mit den Daten sehr bewusst. Bei der „Zentralkartei" handelt es sich wohl um eine reine Adressdatei. In den Gesundheitsämtern gibt es auch Zugriffs- und Berechtigungskonzepte, allerdings keine einheitlichen landesweiten Vorgaben hierzu.
Große Unsicherheiten bestehen aber in Bezug auf die Notwendigkeit des Löschens der Daten. Nicht eindeutig klar ist, welche Daten für die Dauer der ärztlichen Aufbewahrungsfrist zu speichern sind und welche Daten nicht hierunter fallen. Hier war ein sehr großer Bedarf an verbindlichen Regelungen festzustellen.
Eine datenschutzkonforme Lösung des Problems konnte derzeit noch nicht erreicht werden. Der TLfDI wird im nächsten Berichtszeitraum die Datenverarbeitung in mindestens einem Gesundheitsamt vor Ort prüfen und dann gemeinsam mit den Gesundheitsämtern und der zuständigen Aufsichtsbehörde Leitlinien zur Aufbewahrung von Daten im Gesundheitsamt erarbeiten.

Grundsätzlich dürfen Daten nur solange gespeichert werden, wie ihre Vorhaltung für die Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Zu beachten sind aber auch bestehende Aufbewahrungsfristen. Es ist im Gesundheitsamt konkret zu prüfen, welche personenbezogenen Daten unter die ärztliche Aufbewahrungsfrist fallen.

11.50 Auskunft zu und Löschung von Sozialdaten

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI)

und trug vor, sie habe an das Sozialamt eine Anfrage gerichtet und Anträge nach dem Landesdatenschutzgesetz gestellt. Sie wollte die Rechtsgrundlagen und den Sachzweck der Speicherung ihrer personenbezogenen Daten im Zusammenhang mit einem Vorgang wissen, der ihren von ihr getrennt lebenden Ehemann betraf. Gleichzeitig hatte sie die Löschung aller sie betreffenden Daten, die ohne Rechtsgrundlage verarbeitet werden, beantragt. Hierauf habe sie keine Antwort erhalten.

Das Sozialamt teilte auf Nachfrage des TLfDI zunächst mit, es könne leider keine Antwort geben, denn die Akte befände sich aufgrund eines Rechtsstreits beim Sozialgericht. Da sich gerichtliche Streitigkeiten über einen längeren Zeitraum ziehen können, bat der TLfDI nach geraumer Zeit um Sachstandsmitteilung. Da der Abschluss des Verfahrens nicht einzuschätzen war, forderte das Sozialamt die Akte vom Sozialgericht an und nahm gegenüber dem TLfDI Stellung. Danach gestaltete sich die Angelegenheit so, dass für den Ehemann Leistungen nach dem Sozialgesetzbuch beantragt waren. Ob die Ehegatten nun getrennt lebten und ab wann, sollte geklärt werden, weil dies maßgeblich zur Berechnung des Bedarfs war. Dies war gegenüber dem TLfDI schlüssig dargelegt worden. Außerdem teilte das Sozialamt mit, die Beschwerdeführerin, die auch gerichtlich vor einiger Zeit zur Betreuerin ihres Ehemannes bestellt worden war, habe aktenkundig Einsicht in die Akte genommen.

Der TLfDI teilte der Beschwerdeführerin daraufhin mit, dass sie mit der Akteneinsicht vollumfänglich Auskunft zu den zu ihrer Person verarbeiteten Daten erhalten habe und damit auch die Rechtsgrundlagen der Verarbeitung ihrer personenbezogenen Daten aus der Akte entnehmen konnte. Da die Darlegung des Sozialamts zur Datenverarbeitung nach den sozialgesetzlichen Vorschriften schlüssig war, wurde sie gebeten, konkret darzulegen, welche Daten denn aus ihrer Sicht unrichtig oder nicht mehr erforderlich seien, sodass sie nach § 84 Sozialgesetzbuch (SGB) Zehntes Buch (X) zu löschen oder zu sperren wären. Allein der Grund, dass Ehegatten zwischenzeitlich getrennt leben oder geschieden sind, macht die Datenverarbeitung nicht unzulässig oder unrichtig. Auch ist sehr fraglich, ob die bereits erhobenen Daten damit zur Aufgabenerfüllung nicht mehr erforderlich sind und aus diesem Grund einem Löschungsanspruch unterliegen könnten. Schließlich ist zu beachten, dass Sozialakten das behördliche Handeln widerspiegeln und nach Abschluss einer Aufbewahrungsfrist unterfallen. Entfallen Ansprüche oder ändern sich die

Lebensumstände, sind nicht automatisch frühere Sachverhalte zu löschen. Ob die Daten eines inzwischen vom Leistungsempfänger getrennten Ehegatten gelöscht werden müssen oder einer Sperrung unterfallen und damit einer Nutzungsbeschränkung unterliegen, ist im Einzelfall zu beurteilen.
Sobald die Beschwerdeführerin ihr Anliegen konkretisiert, wird der TLfDI der Angelegenheit weiter nachgehen.

Nach § 84 SGB X sind Sozialdaten zu berichtigen, wenn sie unrichtig sind. Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Allein die Änderung des Familienstandes macht die Verarbeitung von personenbezogenen Daten des von einem Sozialleistungsempfänger getrennten Ehepartners grundsätzlich noch nicht unzulässig.

11.51 Thüringer Verordnung über die statistischen Angaben für die Gleichstellung von Frauen und Männern nach dem Thüringer Gleichstellungsgesetz

Das (damalige) Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) stellte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) am Ende des Berichtszeitraumes des 10. Tätigkeitsberichtes den Entwurf der Thüringer Verordnung über die statistischen Angaben für die Gleichstellung von Frauen und Männern in Dienststellen des Freistaats Thüringen (Thüringer Gleichstellungsstatistikverordnung – ThürGleichStatVO) mit der Bitte um summarische Prüfung zur Verfügung. Gleichzeitig bat das TMSFG den TLfDI um Mitteilung, ob Bedenken gegen den genannten Verordnungsentwurf aus datenschutzrechtlicher Sicht bestünden. Nach Information des TMSFG sollte die nach § 5 Abs. 2 Thüringer Gleichstellungsgesetz vorgesehene Anhörung des TLfDI nach Abschluss der Ressortabstimmung erfolgen. Der TLfDI nahm zum Entwurf der ThürGleichStatVO Stellung und merkte aus datenschutzrechtlichen Gesichtspunkten eine Vielzahl von kritischen Textpassagen an.
So teilte der TLfDI dem TMSFG beispielsweise mit, dass nicht für alle der nach § 1 Abs. 2 Nr. 6 bis 8 der Verordnung statistisch zu erfassenden Daten das Thüringer Gleichstellungsgesetz als Ermächtigungsgrundlage herangezogen werden könne und bat in Folge, den jeweiligen Passus in der Verordnung zu streichen.

Nach der Ressortabstimmung übersandte das TMSFG dem TLfDI wiederum den Entwurf der ThürGleichStatVO mit der Bitte um datenschutzrechtliche Stellungnahme. Der TLfDI musste nach Prüfung feststellen, dass seine kritischen Anmerkungen zum vorherigen Entwurf nicht in Gänze übernommen worden waren, sodass diese Punkte aus datenschutzrechtlicher Sicht erneut kritisiert wurden.
Zum Berichtszeitraumende stellte das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) dem TLfDI im Rahmen der Anhörung nach §§ 20, 21 Gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen (ThürGGO) den ressortabgestimmten Entwurf eines Ersten Gesetzes zur Änderung des Thüringer Gleichstellungsgesetzes und den ressortabgestimmten Entwurf der ThürGleichStatVO zur Verfügung. Der TLfDI hatte an diesen nichts mehr zu kritisieren, da seine unterbreiteten Anregungen nunmehr Eingang gefunden hatten.

Die Thüringer Gleichstellungsstatistikverordnung regelt die Erhebung geschlechtsspezifischer Daten zur Beschäftigung in der Landes- und Kommunalverwaltung. Diese Daten sind Grundlage für den von der Landesregierung nach § 14 des Thüringer Gleichstellungsgesetzes alle sechs Jahre zu erstellenden Erfahrungsbericht über die Gleichstellung von Frauen und Männern in den Dienststellen des Freistaates Thüringen. Darüber hinaus dienen die auf der Grundlage dieser Rechtsverordnung erhobenen Daten den personalführenden Dienststellen als Grundlage für die nach § 4 des Thüringer Gleichstellungsgesetzes zu erstellenden Gleichstellungspläne.
Die Anregungen des TLfDI zur Verordnung wurden umgesetzt, sodass diese den datenschutzrechtlichen Bestimmungen genügt.

11.52 Auskünfte über Kontenbewegung

Ein Antragsteller für die Grundsicherung für Arbeitsuchende, auch Arbeitslosengeld (ALG) II oder Hartz IV genannt, beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine vom Jobcenter veranlasste Kontenabfrage bei seiner Bank. In diesem Zusammenhang bat er den TLfDI auch um Mitteilung, ob das Jobcenter die Vorlage von ungeschwärzten Kontoauszügen verlangen darf. In seiner Antwort verwies der TLfDI den Beschwerdeführer zunächst darauf, dass dem

Antragsteller nach § 60 Abs. 1 Sozialgesetzbuch (SGB) Erstes Buch (I) bei der Beantragung von Sozialleistungen eine Mitwirkungspflicht obliegt. Danach hat jeder, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte von Seiten Dritter zuzustimmen und Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen. Klare Vorgaben, welche Angaben gegebenenfalls vom Antragsteller auf Kontoauszügen oder anderen Unterlagen geschwärzt werden dürfen, lassen sich dem Gesetz leider nicht entnehmen. Um sowohl dem Recht auf informationelle Selbstbestimmung des Antragstellers als auch den Interessen des Sozialleistungsträgers angemessen Rechnung tragen zu können, sollte die Anforderung von Kontoauszügen zum Zwecke der Klärung einer konkreten Frage zu der Einkommens- und Vermögenssituation der Hilfesuchenden erforderlich sein, weil sie nicht mit der Vorlage anderer Unterlagen herbeigeführt werden kann oder weil konkrete Zweifel an der Vollständigkeit oder Richtigkeit der Angaben der Hilfesuchenden bestehen. Insbesondere bei Soll-Buchungen über geringere Beträge (regelmäßig bis 50 Euro) kann der Hilfesuchende die zu den Einzelbuchungen aufgeführten Texte in der Regel schwärzen. Der Betrag selbst muss sichtbar bleiben. Schwärzungen können unabhängig vom Betrag grundsätzlich dann vorgenommen werden, wenn die Buchungstexte Angaben über besonders geschützte Daten im Sinne des § 67 Abs. 12 SGB Zehntes Buch (X) enthalten. Dazu zählen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Beispielweise kann bei Überweisungen von Mitgliedsbeiträgen an eine Partei bzw. eine Gewerkschaft oder bei Zahlungen an eine Religionsgemeinschaft die Bezeichnung der Organisation geschwärzt werden. Der Text „Mitgliedsbeitrag“ oder „Spende“ sollte lesbar bleiben, um Missverständnisse zu vermeiden. Hält das Jobcenter es in Einzelfällen für erforderlich, bestimmte Einzelbuchungen ungeschwärzt zur Kenntnis zu nehmen, ist dies gegenüber dem Betroffenen zu begründen. Dem hingegen kann das Schwärzen von Haben-Buchungen, also von Einnahmen, zu einer Verletzung der Mitwirkungspflicht führen, da grundsätzlich das gesamte Einkommen bei der Hilfegewährung zu berücksichtigen ist. Die Verpflichtung zur Vorlage von

Kontoauszügen gemäß § 60 SGB I stellt allerdings keine Befugnis zur Speicherung dieser Daten dar. Vielmehr dürfen diese nur dann gespeichert werden, wenn die Daten zur Aufgabenerfüllung im Einzelfall erforderlich sind. Grundsätzlich reicht es aus, wenn das Jobcenter in den Akten vermerkt, dass die Kontoauszüge vorgelegen haben und hieraus keine Anhaltspunkte für einen Leistungsmissbrauch ersichtlich sind. Der TLfDI forderte vom Jobcenter eine Stellungnahme, aus welchen Gründen dort bei einer Bank Kontendaten über den Betroffenen erhoben wurden. Wie aus dem Antwortschreiben hervorging, stützte das Jobcenter sein Auskunftsersuchen an die Bank auf Regelungen des § 21 Abs. 1 S. 1 SGB Zweites Buch (II). Die Regelung erlaubt der Behörde, sich der Beweismittel zu bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält, wobei sich aus den materiellen Anforderungen des jeweiligen Fachrechts ergibt, welche Maßnahmen zur Beweisermittlung erforderlich sind. Im vorliegenden Fall hatte das Jobcenter ein Kontoabrufersuchen eingeleitet, worüber der Beschwerdeführer unterrichtet wurde. Das Bundeszentralamt für Steuern hatte daraufhin dem Jobcenter die Konten des Beschwerdeführers mitgeteilt. Daraufhin wurde der Betroffene zur Vorlage von Kontoauszügen aufgefordert, der dieser Forderung jedoch nicht nachkam. Der TLfDI teilte dem Beschwerdeführer abschließend mit, dass im begründeten Einzelfall ein Jobcenter bei einer Bank Kontendaten des Antragstellers erheben kann. Die Banken und Sparkassen müssen gemäß § 60 Abs. 2 SBG II Auskunft über Guthaben oder verwahrte Vermögensgegenstände erteilen. Grundsätzlich sind nach § 67a Abs. 2 SGB X die für den Antrag benötigten Daten beim Antragssteller zu erheben. Sind die Informationen, die bei der Antragsstellung vorliegen, nach Auffassung der Behörde nicht ausreichend, muss der Antragssteller aufgefordert werden, weitere Angaben zu machen und diese gegebenenfalls zu belegen. Wie der TLfDI feststellte, war diese Anfrage mit einem Schreiben des Jobcenters an den Antragsteller erfolgt. Weil dieser jedoch die von der Behörde verlangten Informationen nicht erteilte und diese Angaben aber für den TLfDI nachvollziehbar zur Durchführung der Aufgaben des Jobcenters erforderlich waren, durfte das Jobcenter nach § 60 Abs. 2 S. 1 SGB II bei der Bank den Kontostand bzw. die Kontoumsätze für den maßgeblichen Zeitraum erfragen.

Ein Antragsteller hat die zur Antragsbearbeitung der Grundsicherung von Arbeitssuchenden nach SBG II erforderlichen Angaben zu erteilen. Hierzu kann auch die Vorlage von Kontoauszügen gegenüber dem Jobcenter gehören. Alle Daten auf diesen Kontoauszügen, die nicht unbedingt als Nachweis erforderlich sind, dürfen vom Antragsteller geschwärzt werden. Erteilt der Antragsteller jedoch keine Informationen über die von ihm geführten Konten, darf das Jobcenter über eine zentrale Anfrage Informationen darüber enthalten, bei welchen Banken Konten des Betroffenen geführt werden. Kommt der Betroffene seiner Auskunftspflicht hierüber nicht nach, darf das Jobcenter sich an die betroffenen Geldinstitute wenden und dort die zur Aufgabenerfüllung erforderlichen Kontodaten erheben.

11.53 Digitalisierung von Akten im Schwerbehindertenrecht

Ein Landratsamt teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass es beabsichtige, die Akten im Schwerbehindertenrecht zu digitalisieren und fragte an, unter welchen Bedingungen dies aus datenschutzrechtlicher Sicht zulässig ist. In seiner Antwort verwies der TLfDI zunächst darauf, dass das Schwerbehindertenrecht im Sozialgesetzbuch (SGB) geregelt ist, weswegen für die datenschutzrechtliche Bewertung das SGB maßgeblich ist. Nach § 78a SGB Zehntes Buch (X) hat die Akten führende Stelle die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Anforderungen des SGB, insbesondere die in der Anlage zu § 78a SGB X genannten acht Anforderungen, zu gewährleisten. Ebenfalls ist herauszustellen, dass das Sozialgeheimnis nach § 35 SGB Erstes Buch sowohl gegenüber Dritten als auch innerhalb der verantwortlichen Stelle gewahrt bleibt. Daher ist zu gewährleisten, dass nur die Personen, die dazu befugt sind, Zugriff auf die Sozialdaten haben. Für die Digitalisierung der Schwerbehindertenakten muss ein eigenes IT-Sicherheitskonzept nach den Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) erstellt werden. Empfohlen wird, wie auf der Seite https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html beschrieben vor-

zugehen und zunächst den Bedarf an Informationssicherheit anhand der festgestellten IT-Grundschutzstufe zu ermitteln, um dann anhand einer Risikoanalyse mögliche Sicherheitsmängel festzustellen und die erforderlichen Maßnahmen zur Risikominimierung schriftlich in Form von Dienstanweisungen festzulegen. Der TLfDI geht dabei davon aus, dass man sich im Bereich des Schwerbehindertenrechts durchweg in der Schutzstufe „hoch“ bis „sehr hoch“ bewegt. Im Internetangebot des BSI sind die BSI-Standards zum IT-Grundschutz unter den Stichwörtern IT-Grundschutz – IT-Grundschutz-Standards sowie die aktuelle Version der IT-Grundschutz-Kataloge unter IT-Grundschutz – IT-Grundschutz-Kataloge zu finden. Die nach dem Baukastenprinzip gegliederten IT-Grundschutz-Kataloge umfassen vom BSI kontinuierlich aktualisiertes Wissen, mit dem die in den BSI-Standards enthaltenen allgemeinen Empfehlungen zum Management von Informationssicherheit in der für die Verarbeitung von Sozialdaten verantwortliche Behörde umgesetzt werden können. In jedem Fall sollten die digitalisierten Daten auf dem Server gemäß der Anlage zu § 78a SGB X mit dem Stand der Technik entsprechenden Verschlüsselungsverfahren verschlüsselt werden. Zudem ist ein Zugriffs- und Berechtigungskonzept zu erstellen, das auch die Mandantenfähigkeit gewährleistet. Die Orientierungshilfe „Mandantenfähigkeit“ des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist unter: https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_mandantenfaehigkeit.pdf zu finden. Weiterhin ist zum Beispiel auch festzulegen, auf welche Weise die Daten vor einem unbefugten Zugriff von außen geschützt werden (Beschaffenheit der Serverräume, Einsatz von Firewalls etc.). Auch muss festgelegt werden, wie sichergestellt wird, dass andere Mitarbeiter beim Scanvorgang keine Kenntnis der Sozialdaten erhalten. Wichtig ist auch, Regelungen dazu zu treffen, wie mit den auf dem Kopierer gespeicherten Scans umzugehen ist. Weiterhin ist zu prüfen, ob die Originaldokumente möglicherweise noch zu Beweiszwecken benötigt werden. In diesem Fall dürfen die Originaldokumente nicht vernichtet werden oder sie müssen mit einer qualifizierten elektronischen Signatur eingescannt werden, da nur dann die Authentizität der Dokumente gewährleistet

ist. Mit dieser Beratung war das Landratsamt zunächst zufrieden. Ihm wurde angeboten, sich bei weiteren Fragen wieder an den TLfDI zu wenden.

Bei der Verarbeitung und Nutzung von Sozialdaten sind nach den Regelungen des § 78a SGB X und der Anlage zahlreiche technische und organisatorische Maßnahmen von der verantwortlichen Stelle zu treffen, um die Ausführungen der Vorschriften dieses SGB zu gewährleisten. Aufgrund des hohen bis sehr hohen Schutzbedarfs der Daten, dem Sozialdaten im Schwerbehindertenrecht unterliegen, sind Maßnahmen besonders sorgfältig auszuwählen.

11.54 Todesursachenrecherche

Im Rahmen einer großangelegten, bundesweiten Studie zur Gesundheit Erwachsener in Deutschland bat das die Studie durchführende Institut die Datenschutzbeauftragten des Bundes und der Länder um ihre datenschutzrechtliche Einschätzung zur Verfahrensgestaltung. Ein Schwerpunkt der Studie ist die Feststellung von Todesursachen für bereits verstorbene Studienteilnehmerinnen und -teilnehmer. Allerdings wird hierfür auf einen Datenpool zugegriffen, der aus einer vorhergehenden Studie in den Jahren 2008 bis 2011 stammt. Zum damaligen Zeitpunkt war eine Todesursachenrecherche noch nicht vom Forschungszweck umfasst. Aufgrund der Unmöglichkeit, bei den verstorbenen Probanden eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zum Zweck der Todesursachenauswertung einzuholen, war vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu klären, unter welchen Bedingungen das Institut Auskünfte aus den von der unteren Gesundheitsbehörde geführten Toten- und Sektionsscheinen erhalten darf. Der TLfDI teilte dem Institut mit, dass in Thüringen die für den Wohnort des Verstorbenen zuständige untere Gesundheitsbehörde gemäß § 15 Abs. 4 Nr. 2 des Thüringer Bestattungsgesetzes auf Antrag Auskünfte aus Totenscheinen und Sektionsscheinen im erforderlichen Umfang erteilen kann. Voraussetzung ist, dass der Antragsteller, hier also das Institut, die Angaben für ein wissenschaftliches Forschungsvorhaben benötigt und das für das Gesundheitswesen zuständige Ministerium festgestellt hat, dass ein öffentliches Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt

und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann. Dem Institut wurde deshalb mitgeteilt, sich zunächst an das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) zu wenden und sich dort bescheinigen zu lassen, dass ein öffentliches Interesse an der Durchführung des wissenschaftlichen Forschungsvorhabens besteht. Das TMASGFF hat die Auffassung des TLfDI in seiner Stellungnahme an das Forschungsinstitut einbezogen.

Forschungsinstitute dürfen von den örtlichen Gesundheitsämtern Auskunft aus Toten- und Sektionsscheinen erhalten, wenn dies zur Durchführung einer im öffentlichen Interesse liegenden wissenschaftlichen Forschungsarbeit erforderlich ist, das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen das Forschungsinteresse nicht überwiegt und der Forschungszweck nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann. Das öffentliche Interesse ist dabei durch das für Gesundheitswesen zuständige Ministerium festzustellen.

11.55 Vaterschaftsfeststellung durch das Jobcenter?

Eine junge Mutter stellte beim Jobcenter den Antrag auf eine Babyerstausstattung. Zu dem Antrag gehörte auch eine Erklärung, dass die Antragstellerin keinen Unterhalt für das Kind erhalte und auch nicht eingefordert habe, weil keine Vaterschaftsanerkennung vorliege. Daraufhin forderte das Jobcenter die Antragstellerin auf, die Adressdaten des Kindsvaters anzugeben. Im Verlauf des Gesprächs im Jobcenter stellte die Antragstellerin fest, dass sich in den Händen des Sachbearbeiters bereits ein Dokument befand, das Adressdaten des vom Jobcenter offenbar vermuteten Vaters enthielt. Dass hinter ihrem Rücken die Daten zum vermeintlichen Vater recherchiert wurden, fand die Antragstellerin nicht in Ordnung und wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Auf die Nachfrage des TLfDI nach der Rechtsgrundlage der Datenerhebung über den vermeintlichen Kindsvater teilte das Jobcenter mit, man habe bei der Prüfung des Antrags auf Leistungen zur Erstausstattung bei Schwangerschaft und Geburt nach § 24 Abs. 3 Sozialgesetzbuch (SGB) Zweites Buch (II) festgestellt, dass zwischen

den Konten der Beschwerdeführerin und einer männlichen Person Gelder flossen. Weil nun der Verdacht aufkam, dass die Betroffene mit dieser Person vielleicht eine Bedarfsgemeinschaft bildete, deren Vorliegen bei der Prüfung der Hilfsbedürftigkeit nach dem SGB II Auswirkungen haben könnte, habe man pflichtgemäß eine Melderegisterabfrage durchgeführt. Als Grundsicherungsträger nach dem SGB II sei das Jobcenter verpflichtet, Sachverhalte von Amts wegen soweit zu ermitteln, dass alle für den Einzelfall bedeutsamen Umstände in die Bedarfsberechnung einfließen.
Fest steht, dass, soweit eine Unterhaltspflicht des Kindsvaters besteht, diese bei der Babyerstausstattung durch das Amt zu berücksichtigen ist, denn eine Hilfsbedürftigkeit liegt nur dann vor, wenn der Unterhaltspflichtige nicht herangezogen werden kann. Bildet die Kindsmutter mit einer anderen Person eine Bedarfsgemeinschaft, ist dies ebenfalls bei der Hilfsbedürftigkeit zu berücksichtigen. Zu diesem Zweck kann das Jobcenter eine Melderegisterauskunft einholen, um festzustellen, ob dieselben Wohnadressen vorliegen.
Nach der Darlegung des Jobcenters war kein datenschutzrechtlicher Verstoß festzustellen. Die einfache Melderegisterauskunft zu einer männlichen Person, von der die Antragstellerin Geldmittel erhalten hatte, war von den Amtsermittlungen gedeckt. Dass damit der Versuch einer Vaterschaftsfeststellung verbunden gewesen wäre, konnte aus dem Sachverhalt nicht entnommen werden.

Der Grundsicherungsträger ist verpflichtet, von Amts wegen zu prüfen, ob und in welcher Höhe ein Anspruch auf Leistungen nach dem SGB II besteht. Bestehende Unterhaltsansprüche können die Hilfsbedürftigkeit vermindern oder entfallen lassen. Bestehen Anhaltspunkte dafür, dass Hilfsbedürftige in einer Bedarfsgemeinschaft leben, ist auch dies zu berücksichtigen. Eine Melderegisterabfrage in diesem Zusammenhang ist nicht unzulässig.

11.56 Jugendberufsagenturen und Datenschutz

Um den Übergang von der Schule in eine Ausbildung und in einen Beruf zu begleiten, wurden bundesweit flächendeckend Jugendberufsagenturen eingerichtet, die für unter 25-Jährige Leistungen nach den Sozialgesetzbüchern Zweites Buch – „Grundsicherung für Arbeitssuchende“, Drittes Buch – „Arbeitsförderung“ und Achtes Buch – „Kinder- und Jugendhilfe“ bündeln sollen. Aus der Aufga-

benbündelung der Jugendberufsagenturen ergibt sich ein Datenaustausch zwischen den daran beteiligten Sozialhilfeträgern sowie den staatlichen Schulen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte erfahren, dass das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) und das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) die Auffassung vertraten, dass Datenübermittlungen zwischen den Schulen und den Jugendberufsagenturen auf der Grundlage der bisher bestehenden gesetzlichen Vorschriften zulässig seien. Dieser Meinung konnte sich der TLfDI jedoch nicht anschließen, weil sich aus dem eindeutigen Wortlaut des § 57 Abs. 4 Thüringer Schulgesetz (ThürSchulG) die Unzulässigkeit einer Übermittlung von Schülerdaten von der Schule an die Jugendberufsagentur ergab. Beide Ministerien wurden dementsprechend vom TLfDI angeschrieben und um Benennung der Rechtsgrundlage gebeten, aus der sich die Zulässigkeit dieser Datenübermittlung ergeben sollte. In einem Antwortschreiben des TMBJS wurde dem TLfDI zugesagt, dass alle erforderlichen Datenübermittlungen von der Schule an die Jugendberufsagenturen ausschließlich auf der Grundlage einer individuellen Einwilligung nach § 57 Abs. 4 Nr. 3 ThürSchulG durch den betroffenen Schüler bzw. dessen Erziehungsberechtigten erfolgen werden. Der TLfDI hatte gegen eine Datenübermittlung mit Einwilligung der Betroffenen keine datenschutzrechtlichen Bedenken. Er wird aber noch prüfen, ob das Einwilligungsverfahren die Voraussetzungen des § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) erfüllt. Hiernach ist der Betroffene auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Der Datenaustausch von personenbezogenen Schülerdaten zwischen den Schulen und den Jugendberufsagenturen ist nach der gegebenen Rechtslage ausschließlich auf der Grundlage einer Einwilligung nach § 57 Abs. 4 Nr. 3 ThürSchulG in Verbindung mit § 4 Abs. 3 ThürDSG zulässig.

11.57 Datenerhebung bei Minderjährigen nur mit Einwilligung der Eltern?

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Wirtschaftsfördervereins zur Erstellung einer Homepage. Diese geplante Homepage des Wirtschaftsfördervereins sollte eine Datenbank mit wesentlichen personenbezogenen Daten wie Namen, Alter, Wohnort, Durchschnittsnote, Interessenfelder sowie Kontaktmöglichkeiten wie E-Mail oder Handynummer zu einer angemeldeten Person und für Dritte, im Regelfall Unternehmen, abrufbar bzw. einsehbar führen. Das Angebot wollte der Wirtschaftsförderverein an Jugendliche und junge Erwachsene ab der 10. Klasse richten. Zugriff auf die Datenbank sollten Unternehmen haben, die auf der Suche nach Fachkräften waren.

Der TLfDI teilte dem Wirtschaftsförderverein mit, dass die angedachte Datenbank unter datenschutzrechtlichen Gesichtspunkten nicht ohne größeren Aufwand realisiert werden könnte. Neben der Erhebung von Daten ist das Erstellen einer Homepage zwangsläufig auch mit der Speicherung und Übermittlung (Verarbeitung) personenbezogener Daten verbunden. Grundsätzlich ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, soweit das BDSG oder eine andere datenschutzrechtliche Vorschrift dies erlaubt oder der Betroffene (in die konkrete Art des Umgangs) eingewilligt hat. Juristisch wird dies als Verbot mit Erlaubnisvorbehalt bezeichnet.

Für den TLfDI war die einzig praktikable und mit dem BDSG vereinbare Lösung für den geplanten Umgang des Wirtschaftsfördervereins mit personenbezogenen Daten, die Einwilligung jedes einzelnen Betroffenen in die Datennutzung einzuholen. Diese muss den Voraussetzungen des § 4a BDSG entsprechen. Jedoch muss für die Wirksamkeit der Einwilligung von Minderjährigen eine Urteils- und Einsichtsfähigkeit des Betroffenen vorhanden sein, die es erlaubt, Grundrechte selbstständig wahrzunehmen bzw. auf deren Ausübung zu verzichten. Dies ist im Falle der informationellen Selbstbestimmung regelmäßig erst ab einem Alter von frühestens 14 Jahren möglich, weswegen eine Nutzung des Angebots für Kinder nur mit Einwilligung der Eltern möglich wäre. Schließlich hat der TLfDI den Wirtschaftsförderverein noch darauf hingewiesen, dass gemäß § 13

Abs. 2 Nr. 2 Telemediengesetz (TMG) die Einwilligung zu protokollieren ist.
Eine andere Erlaubnisnorm für das Vorhaben des Wirtschaftsfördervereins außer der vorgenannten Einwilligung der Betroffenen war nach Überprüfung der Sach- und Rechtslage vom TLfDI nicht ersichtlich. Soweit ersichtlich, hat der Verein die Idee der geplanten Datenbank verworfen.

Für die Wirksamkeit der Einwilligung von Minderjährigen in den Umgang mit personenbezogenen Daten muss eine Urteils- und Einsichtsfähigkeit des Betroffenen vorhanden sein, die es erlaubt, Grundrechte selbstständig wahrzunehmen bzw. auf deren Ausübung zu verzichten. Dies ist im Falle der informationellen Selbstbestimmung regelmäßig erst ab einem Alter von frühestens 14 Jahren möglich. Vor Erreichen dieser Altersgrenze, die im Einzelfall auch höher liegen kann, bedarf es der Einwilligung der Erziehungsberechtigten.

11.58 Sperren statt löschen

In der Eingabe eines Bürgers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete dieser, dass er im Zusammenhang mit seiner Teilnahme an einer Eingliederungsmaßnahme in den Arbeitsmarkt gegenüber dem die Maßnahme durchführenden Berufsförderungszentrum zahlreiche Daten zu seiner Person angeben musste und nunmehr nach Ende der Maßnahme dort die sofortige Löschung der ihn betreffenden Daten begehrte. Dieser Forderung sei jedoch das Berufsförderungszentrum nicht nachgekommen. Der TLfDI schrieb daraufhin die genannte Stelle an und bat um Stellungnahme zum Sachverhalt. Das Berufsförderungszentrum teilte dem TLfDI mit, dass die Stelle als Bildungsträger aufgrund vertraglich vorgegebener Aufbewahrungsfristen zur Prüfung der qualitätsgerechten Umsetzung von Ausschreibungsmaßnahmen „Arbeitsmarkt-Dienstleistungen“ nicht berechtigt sei, Daten von Teilnehmern vor Erreichen einer Zwei-Jahres-Frist zu löschen. Die Stelle sei verpflichtet, den Weisungen des Jobcenters zum Umgang mit den Daten nachzukommen. Der TLfDI wies das Berufsförderungszentrum auf die Regelung des § 20 Abs. 3 Nr. 1 Bundesdatenschutzgesetz (BDSG) hin, wonach, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, an die Stelle einer Löschung eine

Sperrung tritt. Wie sich im Nachhinein ergab, verarbeitet das Berufsbildungszentrum jedoch als Auftragnehmer für das Jobcenter Sozialdaten, sodass die Sperrung nach der praktisch wortgleichen Regelung des § 84 Abs. 3 Nr. 1 SGB X zu erfolgen hatte. Der TLfDI forderte die Stelle auf, ihn über die erfolgte Sperrung zu unterrichten und einen entsprechenden Nachweis hierüber vorzulegen. Das Berufsförderungszentrum wurde darüber hinaus ersucht, alle Kopien der Daten auf Arbeitsplatz-PCs zu löschen, soweit die Kenntnis für die Mitarbeiter zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Der Beschwerdeführer wurde abschließend über die zweijährige Aufbewahrungsfrist seiner dort gespeicherten Daten und die vom TLfDI geforderte Sperrung seiner Daten unterrichtet. Das Berufsförderzentrum teilte auf die vom TLfDI geforderte Sperrung der Daten des Beschwerdeführers mit, dass die automatisiert verarbeiteten Daten verschlüsselt abgelegt und die notwendigen Passwörter zur Entschlüsselung in einem Panzerschrank hinterlegt seien, zu dem lediglich zwei Personen Zugang haben. Alle in Papierform gespeicherten Unterlagen, die personenbezogene Daten des Beschwerdeführers enthalten, befinden sich in einem Archiv der Stelle unter Verschluss. Weitere Kopien dieser Daten seien in der Stelle nicht gespeichert worden. Nach Prüfung der erneuten Stellungnahme des Berufsförderzentrums kam der TLfDI zu dem Ergebnis, dass die Sperrung der Daten des Beschwerdeführers glaubhaft nachgewiesen wurde. Allerdings fragte der TLfDI nach Beendigung der Aufbewahrungsfrist bei der Stelle nochmals an, ob denn nunmehr die Daten des Bürgers gelöscht wurden. Nach Auskunft der Stelle sei der Teilnehmer vorzeitig aus der Bildungsmaßnahme ausgeschieden. Die zweijährige Aufbewahrungsfrist beginne jedoch erst mit Ablauf des tatsächlichen Ablaufs der Maßnahme, sodass die in Rede stehenden Daten noch nicht gelöscht werden dürften. Der TLfDI widersprach der Stelle und wies auf den zwischen der Stelle und der Bundesagentur für Arbeit geschlossenen Vertrag hin, wonach die zweijährige Aufbewahrung eine Maximalfrist ist. Im Falle des Beschwerdeführers war nicht ersichtlich, wieso eine längere Aufbewahrungsfrist seiner Daten erforderlich sein sollte. Nach § 84 Abs. 2 Satz 2 SGB X sind personenbezogene Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zur Annahme besteht, dass durch die Löschung schutzwürdige Interessen

des Betroffenen beeinträchtigt werden. Der Vorgang konnte im vorliegenden Berichtszeitraum noch nicht abgeschlossen werden, da eine erneute Stellungnahme des Berufsbildungszentrums noch nicht vorlag. Der TLfDI wird aber auf eine schnelle Löschung der Daten des Bürgers dringen.

Nach § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Nach § 84 Abs. 3 Nr. 1 SGB X tritt an die Stelle einer Löschung eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

11.59 Mütter und Hebammenleistungen – Befragung „entbindet“ nicht von Datenschutz

Das ehemalige Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um dessen datenschutzrechtliche Stellungnahme zu einer geplanten Mütterbefragung. Hintergrund hierfür war die Erstellung eines Gutachtens des TMSFG zur Beantwortung der Frage, inwieweit sich das vom Hebammenlandesverband sowie von verschiedenen Thüringer Bürgerinnen vorgetragene medizinische Versorgungsproblem mit Hebammenleistungen tatsächlich darstellt. Zu diesem Zweck plante das TMSFG eine Mütterbefragung in Thüringen unter Verwendung eines Erhebungsbogens. Um diesen Fragebogen gemäß einer Stichprobenvorgabe einem ausgewählten Personenkreis von Müttern zukommen lassen zu können, hatte das TMSFG an das damalige Thüringer Innenministerium (TIM) ein Auskunftsersuchen nach § 34 Abs. 1 Satz 2 Nr. 4b des Thüringer Meldegesetzes gerichtet. Auf diese Weise sollten die Adressen aller Haushalte in Thüringen nach einer vorherigen Gemeindeauswahl ermittelt werden, in denen im Jahr 2014 Kinder geboren worden waren. Aus diesen Adressen sollte dann eine zufällige Auswahl getroffen und die Haushalte mit einem Fragebogen zur Zufriedenheit der Mütter mit dem bestehenden Hebammenangebot befragt werden. Die Mütterbefragung war aufgrund

einer fehlenden Rechtsgrundlage, die zur Teilnahme verpflichtete, nur auf freiwilliger Basis zulässig. Gleiches galt für die anonyme Beantwortung des Erhebungsbogens durch die betroffenen Mütter. Da das TIM dem Auskunftsersuchen zunächst nicht nachkam und die Bewertung dieses Auskunftsersuchens auch von der datenschutzrechtlichen Bewertung des TLfDI abhängig machen wollte, erläuterte der TLfDI dem TMSFG die Voraussetzungen für eine Zustimmung durch das TIM. Danach betrieb das Land im Landesrechenzentrum gemäß § 34 Abs. 1 Satz 1 Thüringer Meldegesetz (ThürMeldeG) – wobei das ThürMeldeG seit dem 1. November 2015 keine Gültigkeit mehr hat und nunmehr durch das für alle Bundesländer gültige neue Bundesmeldegesetz abgelöst wurde – ein landeseinheitliches Verfahren für das Meldewesen. Mit anderen Worten lagen dort die Melderegisterdaten aller Thüringer Meldeämter, wobei dies auch nach der Gesetzesänderung gemäß § 5 Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes weiterhin der Fall ist. Nach § 34 Abs. 1 Nr. 4 Buchstabe c ThürMeldeG bedurfte die Erfüllung von Auskunftsersuchen von Behörden oder öffentlichen Stellen der Zustimmung des für das Meldewesen zuständigen Ministeriums. Dem TIM war darzulegen, dass das Auskunftsersuchen die überwiegende Zahl der Meldebehörden betrifft und die Daten direkt bei den Meldebehörden nur mit unverhältnismäßig hohem Aufwand beschafft werden können. Weiterhin musste begründet werden, dass das TMSFG ohne Kenntnis der Daten zur Erfüllung seiner gesetzlichen Aufgaben nicht in der Lage gewesen wäre. Der TLfDI bat zur datenschutzrechtlichen Prüfung der Angelegenheit um Zusendung des Fragebogens und um Angaben dazu, wie sichergestellt wird, dass eine anonymisierte Antwort durch die Teilnehmerinnen an dem Verfahren möglich ist. Personenbezogene Angaben waren für die Untersuchung nicht erforderlich. Darüber hinaus hätten möglicherweise auch weniger Mütter an der Untersuchung teilgenommen. Wie sich herausstellte, sollten die Antworten in den Fragebögen durch ein vom TMSFG beauftragtes privates Forschungsinstitut ausgewertet werden. Der Fragebogen enthielt ein Kürzel des Landkreises oder der kreisfreien Stadt, in der die ausgewählten Mütter wohnten, allerdings keine Namens- oder Adressangabe derjenigen Mütter, die auf freiwilliger Basis bereit waren, den Fragebogen auszufüllen und an das genannte Institut zu senden. Somit war sichergestellt, dass das Institut nur anonymisierte Erhebungsbögen zur Auswertung erhielt. Der TLfDI verlangte vom TMSFG, die aus dem Einwohnermeldere-

gister übermittelten Namens- und Adressdaten rechtssicher zu löschen, nachdem die Erhebungsbögen mit dem Kennzeichen des Landkreises oder der kreisfreien Stadt versehen wurden. Auch sollte nicht automatisch die weibliche Person im Haushalt, sondern neutral der gesetzliche Vertreter des Kindes angeschrieben werden. Der TLfDI hatte im Übrigen keine Bedenken gegen die Durchführung des Erhebungsverfahrens. Wie sich aus einem Schreiben des TMSFG an das TIM ergab, welches dem TLfDI nachrichtlich zur Kenntnis gegeben wurde, versicherte das TMSFG, dass alle vom TLfDI genannten Voraussetzungen eingehalten wurden.

Aus datenschutzrechtlicher Sicht bestand gegen die Übermittlung der Meldedaten an das TMSFG aus den Thüringer Einwohnermelderegistern keine Bedenken, da das Erhebungsverfahren zur Erfüllung der Aufgaben des TMSFG erforderlich war und seitens des Ministeriums die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Bestimmungen des Thüringer Datenschutzgesetzes getroffen wurden.

11.60 Gesundheitsdaten von Asylbewerbern

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom Sozialamt Jena auf eine datenschutzrechtliche Problematik im Zusammenhang mit der Abrechnung von notwendigen ärztlichen Behandlungen gegenüber dem Freistaat Thüringen aufmerksam gemacht.
Gemäß § 4 Asylbewerberleistungsgesetz hat das jeweilige Sozialamt die Kosten der notwendigen Untersuchungen von Asylbewerbern zu übernehmen. Soweit die Kosten für diese notwendigen Untersuchungen einen Betrag von 2556,46 Euro pro Person und Jahr überschreiten, hatte das Sozialamt einen Erstattungsanspruch in Höhe der über diesen Betrag hinausgehenden Kosten nach § 2 Abs. 5 der Thüringer Verordnung über die Kostenerstattung nach dem Thüringer Flüchtlingsaufnahmegesetz (ThürFlüKEVO) gegenüber dem Freistaat Thüringen. Solche Erstattungsansprüche hatte das Sozialamt gegenüber dem Thüringer Landesverwaltungsamt (TLVwA) geltend gemacht, worauf dieses die Übersendung der jeweiligen Krankenakten zur Prüfung angefordert hatte. Auf diese Anfrage des TLVwA meldete sich das Sozialamt Jena beim TLfDI, weil es der Auffassung war, dass die Übersendung der Krankenakten gegen das Thüringer

Datenschutzgesetz (ThürDSG) verstoße. Der TLfDI teilte nach datenschutzrechtlicher Prüfung die Auffassung des Sozialamts Jena. Die Datenerhebung seitens des TLVwA sowie die geforderte Übermittlung der Krankenakten durch das Sozialamt würden einen datenschutzrechtlichen Verstoß darstellen.
Gemäß § 4 Abs. 1 ThürDSG ist eine Verarbeitung oder Nutzung personenbezogener Daten nur dann zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine Einwilligung der Betroffenen lag in diesem Fall nicht vor. Das Erheben personenbezogener Daten ist nach § 19 Abs. 1 ThürDSG zulässig, wenn ihre Kenntnis für die Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Die Übermittlung ist Teil der Datenverarbeitung. Maßgeblich für die Zulässigkeit der hier angedachten Übermittlung ist daher § 21 ThürDSG, der die Übermittlung von personenbezogenen Daten zwischen Behörden regelt. Danach ist eine Übermittlung personenbezogener Daten an eine andere öffentliche Stelle nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten (Empfängers) liegenden Aufgaben erforderlich ist.
Die Erstattung der Kosten nach § 2 Abs. 5 ThürFlüKEVO hat gegen Einzelnachweis zu erfolgen. Das TLVwA ist nach § 4 Abs. 1 ThürFlüKEVO für die Kostenerstattung zuständig. Für den Einzelnachweis in dem mitgeteilten Fall genügt die Übermittlung der der jeweiligen Person zugeordneten Arztrechnungen. Diese müssen erkennen lassen, welche Person behandelt und welcher Betrag dem Fachdienst Soziales in Rechnung gestellt worden ist. Hinsichtlich Diagnose und einzelner Posten sind die Rechnungen jeweils zu schwärzen. Eine Prüfpflicht hinsichtlich der Notwendigkeit der einzelnen Behandlungen durch den Arzt ist von der ThürFlüKEVO nicht vorgesehen und damit für die Aufgabenerfüllung des TLVwA auch nicht erforderlich. Das Sozialamt gab dem TLVwA die Stellungnahme des TLfDI zur Kenntnis. Daraufhin forderte das TLVwA die Weiterleitung amtsärztlicher Stellungnahmen. Die amtsärztlichen Stellungnahmen sind Bestandteil der Krankenhilfeakten und enthalten nach Angaben des Sozialamtes in der Regel zu Diagnosen, Vorerkrankungen und Prognosen oft weitreichendere Angaben als eine Kostenübernahmeanfrage einer Klinik oder eines niedergelassenen Arztes.
Nach Auffassung des TLfDI kann das TLVwA die Vorlage der amtsärztlichen Stellungnahme zwar fordern. Im vorliegenden Fall

war der Inhalt der amtsärztlichen Stellungnahme allerdings viel zu weitgehend. Dem Sozialamt wurde daher empfohlen, die amtsärztliche Stellungnahme zu übermitteln und die Passagen zu schwärzen, die nicht zur Entscheidung des TLVwA über den Erstattungsantrag erforderlich sind. Um derartige Probleme für die Zukunft zu unterbinden, wurde dem Sozialamt dringend empfohlen, die Auftragserteilung an die amtsärztliche Untersuchung zu konkretisieren, um dem Amtsarzt genau mitzuteilen, welche Informationen erfragt werden.

Sowohl die Erhebung von personenbezogenen Daten als auch ihre Übermittlung muss zum Zweck der Aufgabenerfüllung der öffentlichen Stelle erforderlich sein. Auch bei der Beauftragung eines Amtsarztes ist darauf zu achten, dass nur die Information erfragt wird, die für die konkrete Aufgabe erforderlich ist.

11.61 Einwilligungserklärung und damit Verzicht auf Ausübung des Grundrechts der informationellen Selbstbestimmung durch Minderjährige?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bekommt immer wieder Anfragen, ab welchem Alter ein Minderjähriger selbst eine rechtswirksame Einwilligung erteilen kann und dies, ohne dass es auf die Einwilligung der Erziehungsberechtigten ankommt. In diesem Fall fragte ein Unternehmen an, das internetbasierte Lern- und Arbeitsplattformen vertreibt, bei denen sich die Lehrkraft für ihre Schüler entsprechende Apps (Applikationen, also Anwendungssoftware) aus dem Angebot aussucht, die der Unterrichtsgestaltung und -nachbereitung dienen. Die Nutzung dieser Apps ist mit der Verarbeitung und Nutzung personenbezogener Daten der Schüler verbunden. Das Unternehmen sah die Problematik, dass die Schüler in die Verarbeitung und Nutzung ihrer Daten gegebenenfalls nicht wirksam einwilligen können und bat den TLfDI um Vorgaben und Richtwerte, ab wann eine Einwilligung von einem Schüler wirksam vorgenommen werden kann oder ob bis zur Volljährigkeit grundsätzlich immer zusätzlich die Einwilligung der Erziehungsberechtigten eingeholt werden muss. Das Unternehmen bat auch um Auskunft, ob die Einwilligung immer schriftlich erklärt werden müsse oder ob auch andere Lösungen denkbar seien. Zuletzt wurde die Frage aufgeworfen, ob ein Minder-

jähriger wirksam in den Erhalt von Werbe-Newsletters einwilligen kann. Der TLfDI legte dem Unternehmen dar, dass es im Freistaat Thüringen keine konkreten Vorgaben bzw. Richtwerte für Altersstufen gibt, nach denen eine Einwilligung durch den Minderjährigen selbst erfolgen kann. Die Voraussetzungen einer rechtswirksamen Einwilligung richten sich je nach Fallkonstellation nach § 4 Abs. 2 und 3 Thüringer Datenschutzgesetz (ThürDSG) bei der Einholung einer Einwilligung durch eine öffentliche Stelle in Thüringen bzw. nach § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) durch eine nichtöffentliche Stelle mit Sitz in Thüringen. Nach beiden Bestimmungen muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Dies setzt ungeachtet der Frage, ob ein Minderjähriger als nach § 106 Bürgerliches Gesetzbuch in der Geschäftsfähigkeit beschränkte Person überhaupt wirksam einen Vertrag über den Erwerb einer App abschließen kann, keine Geschäftsfähigkeit des Minderjährigen, sondern lediglich dessen Einsichtsfähigkeit in die Tragweite der Einwilligung voraus.

Wann von einer solchen Einsichtsfähigkeit ausgegangen werden kann, lässt sich nicht an abstrakten Altersgrenzen festmachen, sondern bedarf einer Entscheidung im Einzelfall. Die Einsichtsfähigkeit von Minderjährigen dürfte in Abhängigkeit vom Umfang der Erhebung personenbezogener Daten sowie deren Verwendungszweck bei der Nutzung von Apps nur in Ausnahmefällen zu bejahen sein. Zusätzlich war zu berücksichtigen, dass ohne Einwilligung der Eltern wohl der wirksame Vertragsschluss zur Nutzung einer App nicht möglich ist. In der Praxis ist es allerdings gang und gäbe, dass sich Minderjährige Apps aus dem Internet herunterladen, die zu großen Teilen kostenlos sind. Solche Rechtsgeschäfte sind jedoch im Regelfall nicht rechtlich, lediglich vorteilhaft für den Minderjährigen. Deshalb können die Eltern nach Auffassung des TLfDI solche Rechtsgeschäfte ihrer Kinder nachträglich widerrufen. Hierbei handelt es sich aber noch um wenig bearbeitetes Neuland, da bisherige Überlegungen stets nur den finanziellen Aspekt berücksichtigen, das „Bezahlen mit personenbezogenen Daten“ aber außer Acht gelassen wird.

Außerdem wies der TLfDI im vorliegenden Fall darauf hin, dass die erforderliche Schriftform der Einwilligung durch die elektronische Form nach § 3a ThürVwVfG ersetzt werden kann. Dafür benötigt man eine qualifizierte elektronische Signatur nach dem Signaturgesetz. Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung der

Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das Gesetz räumt der Schriftform den unbedingten Vorrang ein. Ausnahmen sind zwar möglich, eine ausdrückliche, das Einverständnis des Betroffenen dokumentierende Erklärung bleibt jedoch unerlässlich. Daher erfüllt eine Lösung mit einer Einwilligung per Web-Formular nicht die gesetzlichen Anforderungen. Da eine pauschale Beantwortung der Frage, ob das Einverständnis der Eltern eingeholt werden muss, nicht möglich ist und dies immer vom gegebenen Einzelfall abhängt, sollten die Erziehungsberechtigten bei Minderjährigen in die Einwilligungserklärung einbezogen werden. Ebenso ist die Frage nach der Wirksamkeit einer Werbeeinwilligung ohne Einverständnis der Erziehungsberechtigten nicht pauschal zu beantworten. Als Beispiel sei auf eine Entscheidung des Oberlandesgerichts Hamm verwiesen, welches feststellte, dass Minderjährige ab 15 Jahren nicht die nötige Reife haben, die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen und daher die Zustimmung der Eltern nötig sei (OLG Hamm, Urteil v. 20. September 2012, I-4 U 85/12).

Es kann kein Alter pauschal angegeben werden, ab dem ein Minderjähriger eine rechtswirksame Einwilligung erteilen kann. Je nach dem konkret vorliegenden Einzelfall ist zu ergründen, ob der Minderjährige die Einsichtsfähigkeit besitzt, die Tragweite seiner Einwilligung für die Verarbeitung und Nutzung seiner personenbezogenen Daten zu erfassen. Dies gilt auch bei Rechtsgeschäften im Zusammenhang mit dem Erwerb von Apps aus dem Internet.

11.62 Anonyme Krankenhäuser

Die datenschutzrechtlichen Probleme in einem Krankenhaus sind wegen der Komplexität der zum Einsatz kommenden Systeme vielfältig. Das stellte auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bei seinen Kontrollen verschiedener Krankenhäuser in Thüringen (vergleiche 10. Tätigkeitsbericht im öffentlichen Bereich, Nummer 11.1) fest. Wegen der Sensibilität der dort verarbeiteten Daten besteht oft eine Scheu, sich an die Aufsichtsbehörde zu wenden, weil eine Frage eventuell schlafende Hunde wecken könnte. Andererseits wusste der TLfDI aus seiner Erfahrung bei den Kontrollen, dass die Kranken-

häuser sehr bemüht sind, sich an die gesetzlichen Vorgaben zu halten. Aus dieser Situation heraus wurde die Idee geboren, ein „anonymes“ Forum für Krankenhäuser zu schaffen. Dieses Forum sollte die Möglichkeit bieten, dass sich Krankenhäuser mit Datenschutzfragen an den TLfDI wenden können, ohne ihre Identität zu offenbaren. Deswegen sollte das Forum auch nicht öffentlich einsehbar, sondern nur den Krankenhäusern in Thüringen zugänglich sein.
Der TLfDI nahm frühzeitig mit der Landeskrankenhausgesellschaft Thüringen e. V. (LKHG) Kontakt auf, um das Vorgehen abzustimmen. Es gestaltete sich nicht ganz einfach, ein Verfahren abzustimmen, das einerseits garantierte, dass nur registrierte Nutzer zu dem Forum Zugang hatten und andererseits aber dem TLfDI die Identität der anfragenden Stelle verborgen blieb. Es wurde der Weg gewählt, dass jedes Krankenhaus in Thüringen einen Zugang erhalten sollte. Die Registrierung der Teilnehmer erfolgte über die LKHG beim Thüringer Landesrechenzentrum (TLRZ). Die Nutzerverwaltung liegt ausschließlich in der Hand des TLRZ. Dieses erhält von der Landeskrankenhausgesellschaft eine Liste der zu registrierenden Benutzerkennungen der Krankenhäuser. Die Benutzerkennungen werden zuvor von der LKHG nach einer bestimmten Regel zufällig vergeben und neben dem TLRZ den an die LKHG gemeldeten Teilnehmern mitgeteilt. Durch die von der LKHG vergebene zufällig kreierte Benutzerkennung werden somit seitens des TLfDI Rückschlüsse auf die anfragende Stelle vermieden. Der Nutzer kann nun eigene und fremde Themen innerhalb des Forums beobachten sowie Themen erstellen, d. h. Fragen an den TLfDI richten. Dabei kann der Nutzer auswählen, ob er gegenüber dem TLfDI mit seinem Benutzernamen oder unter „Anonymous“ auftreten möchte. Damit können sich die Thüringer Krankenhäuser nunmehr bei datenschutzrechtlichen Fragestellungen schnell und unkompliziert an den TLfDI wenden. Die Antworten des TLfDI werden nach Prüfung der Fragen und deren Beantwortung dann im Forum eingestellt und sind für alle Forennutzer lesbar. Am 8. Dezember 2015 startete der TLfDI das Forum in einem gemeinsamen Pressetermin mit der LKHG (siehe auch https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/151209_gem._pm_zur_bloger__ffnung.pdf).

Der TLDI hofft, dass die Krankenhäuser das Forum nutzen werden, um sich mit ihren datenschutzrechtlichen Problemen an ihn zu wenden. Mit dem Forum wünscht sich der TLfDI, das Vertrauen der Betreiber der Krankenhäuser zu gewinnen. Denn datenschutzrechtliche Missstände werden nicht nur kritisiert und beanstandet, diese müssen auch aufgearbeitet und verbessert/abgeschafft werden. Dabei wird der TLfDI die konstruktive Zusammenarbeit mit den Thüringer Krankenhäusern vertiefen. Im nächsten Tätigkeitsbericht wird zu lesen sein, wie die Krankenhäuser das Forum angenommen haben.

Mit dem Krankenhausforum hat der TLfDI eine geschlossene Plattform eingerichtet, auf der sich registrierte und freigegebene Benutzer der Krankenhäuser mit ihren Fragen zum Datenschutz an den TLfDI wenden können, ohne dass dieser über die Identität der anfragenden Stelle Kenntnis erlangt. Damit müssen Datenschutzprobleme nicht „hinter dem Berg“ gehalten werden und alle Nutzer können an der Lösung partizipieren.

Landstraße, Windkraft, Umwelt © mahey / Fotolia.com

12 Infrastruktur und Landwirtschaft

12.1 Bekenntnis zur freiheitlichen demokratischen Grundordnung bei Ausschreibungen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Information, dass das Thüringer Liegenschaftsmanagement in seinen Formularen für die Bieter in Ausschreibungsverfahren folgende Formulierung verwenden würde:

„Mir/uns ist nicht bekannt, dass bei den von mir/uns eingesetzten Mitarbeitern Zweifel am Bekenntnis der betroffenen Person zur freiheitlichen demokratischen Grundordnung bestehen. Mir/uns ist nicht bekannt, dass das eingesetzte Personal Mitglied in einer extremistischen/verfassungsfeindlichen Partei, Organisation oder sonstigen Vereinigung ist bzw. diesen nahesteht und Schriftgut extremistischen oder sonstigen verfassungsfeindlichen Inhalts besitzt und/oder derartiges Schrift- oder Gedankengut weiterverbreitet.“

Der TLfDI bat daraufhin das Thüringer Liegenschaftsmanagement um Stellungnahme, auf welcher Rechtsgrundlage die genannte Erklärung von den Bietern in Ausschreibungsverfahren verlangt wird und inwieweit diese erforderlich ist.
Daraufhin teilte das Thüringer Liegenschaftsmanagement mit, dass der Sachverhalt im damals zuständigen Thüringer Ministerium für Bau, Landesentwicklung und Verkehr (TMBLV) im Wege der Fachaufsicht einer Prüfung unterzogen und bis zum Vorliegen einer Entscheidung des Ministeriums von einer solchen Bietererklärung abgesehen werde. Das Thüringer Liegenschaftsmanagement wollte sich, sobald die Ergebnisse vorliegen, unaufgefordert wieder an den TLfDI wenden. Nachdem der TLfDI jedoch mehrere Monate nichts mehr in der Angelegenheit gehört hatte, wandte er sich erneut an das Liegenschaftsmanagement und erinnerte an dessen Unterstützungspflicht gemäß §§ 38 Abs. 1 Satz 1 und Satz 2 Thüringer Datenschutzgesetz (ThürDSG). Prompt folgte eine Reaktion des Thüringer Liegenschaftsmanagements: In Abstimmung mit dem nunmehr zuständigen Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL) teilte das Thüringer Liegenschaftsmanagement dem TLfDI mit, dass die Bietererklärung schon seit Mitte 2014 keine Verwendung mehr finde und auch zukünftig nicht gefordert werde. Der TLfDI sah damit die Angelegenheit als erledigt an.

Der TLfDI hat Verständnis dafür, dass das Thüringer Liegenschaftsmanagement im Rahmen von Ausschreibungsverfahren nicht mit Bietern in Kontakt treten möchte, deren Bekenntnis zur freiheitlichen demokratischen Grundordnung fragwürdig erscheint. Gleichwohl barg die zunächst verwendete Erklärung die Gefahr, dass konkret personenbeziehbare Daten hier ohne Rechtsgrundlage verarbeitet werden. Dies zu verhindern, ist gemäß § 4 Abs. 1 in Verbindung mit § 37 Abs. 1 ThürDSG die Aufgabe des TLfDI.

12.2 Smarte Heizung – Datenleck?

Das damalige Thüringer Ministerium für Wirtschaft, Arbeit und Technologie fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, wie die Einführung eines intelligenten Heizsystems mit einer selbstlernenden Einzelraumregelung aus datenschutzrechtlicher Sicht zu beurteilen sei. Der TLfDI geht zunächst davon aus, dass das Ministerium als Daten

verarbeitende Stelle im Sinne von § 3 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) für die beim Betrieb des Heizsystems anfallenden Daten verantwortlich ist. Das System erfasst die Anwesenheit und die Dauer der Anwesenheit sowie das Wärmebedürfnis von Personen in den Büroräumen des Ministeriums. Da diese Büros im Regelfall bestimmten Mitarbeitern zugeordnet werden können, entstehen hierbei zumindest personenbeziehbare Daten, die personenbezogenen Daten gleichzusetzen sind (§ 3 Abs. 1 ThürDSG). Die Verarbeitung und Nutzung personenbezogener Daten sind gemäß § 4 Abs. 1 ThürDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder bestimmt oder soweit die betroffene Person eingewilligt hat. Der TLfDI erachtete daher einen Testlauf des Systems im Ministerium mit Einwilligung der betroffenen Mitarbeiter für zulässig. Er hat allerdings ausdrücklich darauf aufmerksam gemacht, dass bei einer späteren allgemeinen und „zwangsweisen“ Einführung des Systems für alle Mitarbeiter sich die Ermächtigungsgrundlage zum Betreiben des Systems nicht mehr aus einer Einwilligung ergeben kann, da diese entgegen der Bestimmung von § 4 Abs. 2 ThürDSG keinesfalls mehr freiwillig erteilt werden würde. Vor einem flächendeckenden Dauerbetrieb des Heizsystems bestehen weiterhin Fragen zur Datensicherheit, die noch nicht beantwortet sind. Diese betreffen z. B. die Sicherheit der Datenübertragung zwischen Raumsensor und Ventilsteuerung sowie die Zugriffssicherheit des Bewegungssensors vor dem unbefugten Auslesen des Anwesenheitsprofils. Nach dem letzten Stand wurde der geplante Testeinsatz des smarten Heizsystems von dem jetzt zuständigen Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft auf unbestimmte Zeit verschoben. Der TLfDI wird die Sache weiter verfolgen.

Die neuen „smarten“ Regeltechniken, bei denen personenbeziehbare Daten entstehen, sind so zu gestalten, dass eine Profilbildung von Personen vermieden wird. Die Einwilligung als Zulässigkeitskriterium scheidet beim Dauerbetrieb eines Regelsystems besonders dann aus, wenn es sich um Bedienstete handelt, da hierbei fraglich ist, ob die Einwilligung in eine vom Dienstherrn eingeführte Regeltechnik tatsächlich freiwillig erteilt wird.

12.3 LPG – nicht datengeschützt

In einer Antwort des ehemaligen Thüringer Ministeriums für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) auf die Kleine Anfrage Nr. 3718 (Drucksache 5/7507) vom 15. März 2014 zu „Unwirksamen Umwandlungen von Landwirtschaftlichen Produktionsgenossenschaften“ hieß es in der Beantwortung der Frage 1 „Liegen der Landesregierung die Namen der betroffenen Betriebe vor?“:
„Die Prüfung durch den Landesdatenschutzbeauftragten ergab, dass eine namentliche Auflistung der 28 unwirksamen Umwandlungen in Thüringen aus datenschutzrechtlichen Gründen nicht möglich war.“
Hintergrund war der datenschutzrechtliche Umgang mit den Angaben zu einzelnen Genossenschaften im Rahmen eines Forschungsprojektes mit dem Titel „Rechtsprobleme der Restrukturierung landwirtschaftlicher Unternehmen in den neuen Bundesländern nach 1989“. In diesem Zusammenhang hatte die frühere Landesbeauftragte für den Datenschutz im Jahr 2001 tatsächlich die Rechtsauffassung vertreten, dass es datenschutzrechtlich nicht vertretbar sei, Einzelangaben zu den betroffenen Landwirtschaftlichen Produktionsgenossenschaften (LPG) zu veröffentlichen.
Hierzu stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nach erneuter datenschutzrechtlicher Prüfung im Berichtszeitraum fest, dass eine Übermittlung personenbezogener Daten, insbesondere die namentliche Auflistung von 28 unwirksam umgewandelten Thüringer Betrieben durch den Leiter des Forschungsprojekts an das TMLFUN aus datenschutzrechtlicher Sicht zulässig sei. Mangels gegenteiliger Hinweise ging der TLfDI davon aus, dass es sich bei den 28 fehlerhaft umgewandelten Thüringer Betrieben um juristische Personen handele. Gemäß § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sowie gemäß § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten aber gerade Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Angaben über juristische Personen und Personenmehrheiten wie Personengesellschaften, Vereine und Gruppen hat der Gesetzgeber bewusst aus dem Anwendungsbereich von BDSG und ThürDSG ausgenommen (vgl. für das BDSG: Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 3, Rz. 18). Juristische Personen sind Personenvereinigungen oder

Zweckvermögen mit vom Gesetz anerkannter rechtlicher Selbstständigkeit.
Folglich unterlagen nach Ansicht des TLfDI die hier infrage stehenden Daten zu den einzelnen früheren LPG nicht dem Schutzbereich des BDSG oder des ThürDSG und konnten daher aus datenschutzrechtlicher Sicht grundsätzlich ohne Weiteres genutzt werden. Diese – revidierte – Rechtsaufassung teilte der TLfDI auch dem TMLFUN mit. Sofern künftig Anfragen an dieses Ministerium zur beschriebenen Problematik herangetragen werden, wird die Rechtsauffassung des TLfDI dort berücksichtigt werden.

Nicht alle Daten werden vom Datenschutzrecht geschützt. Unter den Schutzbereich von § 3 Abs. 1 ThürDSG / § 3 Abs. 1 BDSG fallen nur Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (also jeder lebende Mensch). Die Daten von juristischen Personen oder Personengesellschaften fallen also nicht unter die genannten Regelungen.

12.4 Bodennutzungshaupterhebung

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber, dass er im Rahmen der vom Thüringer Landesamt für Statistik (TLS) durchgeführten Bodennutzungshaupterhebung, einer Agrarstatistik, bei der Abfrage von Flächenveränderungen nach dem Namen und der Anschrift des Flächenabgebers bzw. des Flächenübernehmers gefragt wurde. Diese Vorgehensweise des TLS hielt er für datenschutzrechtlich unzulässig und für eine Statistik unnötig und bat den TLfDI deswegen um Hilfe.
Der TLfDI unterzog den Sachverhalt unter Einbeziehung des TLS einer datenschutzrechtlichen Prüfung und teilte dem Beschwerdeführer Folgendes mit:
Die Bodennutzungshaupterhebung als Bestandteil der Bodennutzungserhebung wird nach Maßgabe des Agrarstatistikgesetzes (AgrStatG) als Bundesstatistik durchgeführt (§ 1 Nr. 1 AgrStatG). Für die Erhebungen zu den Agrarstatistiken nach § 1 AgrStatG besteht gemäß § 93 Abs. 1 AgrStatG Auskunftspflicht. Die Vor- und Familiennamen sowie Anschriften der bisherigen Flächenbewirtschafter sowie der neuen Flächenbewirtschafter oder der jeweiligen Eigentümer

sind nach § 92 Nr. 6 AgrStatG als Hilfsmerkmale bei der Bodennutzungshaupterhebung gesetzlich festgelegt.
Im Ergebnis informierte der TLfDI den Beschwerdeführer, dass das Verarbeiten (dazu zählt auch das Erheben) seiner personenbezogenen Daten gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) datenschutzrechtlich zulässig war, da das Agrarstatistikgesetz (§ 1 Nr. 1 AgrStatG i. V. m. § 92 Nr. 6 AgrStatG) eine derartige Verarbeitung der Daten erlaubt bzw. anordnet. Der TLfDI informierte den Beschwerdeführer ferner darüber, dass die genannten Hilfsmerkmale vom TLS nach abgeschlossener Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit gemäß § 12 Bundesstatistikgesetz zu löschen sind.

Im Rahmen der Bodennutzungshaupterhebung ist bei der Abfrage von Flächenveränderungen das Verarbeiten der personenbezogenen Daten des Flächenabgebers und Flächenübernehmers (Vor- und Familiennamen sowie Anschriften) gemäß § 4 Abs. 1 ThürDSG datenschutzrechtlich zulässig, da das Agrarstatistikgesetz (§ 1 Nr. 1 AgrStatG i. V. m. § 92 Nr. 6 AgrStatG) eine derartige Verarbeitung der Daten erlaubt bzw. anordnet.

12.5 Veröffentlichung personenbezogener Daten in Überwachungsberichten der Immissionsschutzbehörde im Internet

Aufgrund der Anfrage eines behördlichen Beauftragten für den Datenschutz wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass die für den Emissions- und Immissionsschutz zuständigen Thüringer Behörden Überwachungsberichte gemäß § 52a Bundes-Immissionsschutzgesetz in Verbindung mit § 9 Industriekläranlagen-Zulassungs- und Überwachungsverordnung sowie den entsprechenden Anlagen der Verordnung im Internet veröffentlichten. Diese Überwachungsberichte wurden nach der Durchführung einer Vor-Ort-Besichtigung von betroffenen Anlagen erstellt und dann der Öffentlichkeit zur Verfügung gestellt. Außer der Bezeichnung der Anlage selbst wurden auch der Name und die Firmenform des Unternehmens aufgeführt. Hierbei ist nicht auszuschließen, dass dabei auch personenbezogene Daten veröffentlicht werden. Dem Schutz des ThürDSG unterfallen nur personenbezogene Daten. Hierbei

handelt es sich nach § 3 Abs. 1 ThürDSG um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Eine gleiche Regelung findet sich in § 3 Abs. 1 Bundesdatenschutzgesetz. Das bedeutet, dass das Datenschutzrecht grundsätzlich nur auf natürliche Personen und nicht auf juristische Personen anwendbar ist. Juristische Personen können sich allenfalls auf ihr Recht am eingerichteten und ausgeübten Gewerbebetrieb bzw. auf ihr Grundrecht auf Eigentum aus Artikel 14 Grundgesetz berufen. Die diesbezügliche Prüfung unterfällt indes nicht der Zuständigkeit des Datenschutzbeauftragten. Es ist jedoch nicht auszuschließen, dass sich unter den betroffenen Firmen auch Einzelkaufleute befinden. Aus den dem TLfDI zum damaligen Zeitpunkt vorliegenden Unterlagen war nicht eindeutig zu entnehmen, ob es sich bei den aufgeführten Firmen ausschließlich um juristische Personen handelt oder ob hinter den Firmen teilweise auch Einzelkaufleute stehen. Grundsätzlich gilt das so genannte Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 ThürDSG, nach dem die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Aus den einschlägigen Regelungen des Bundesimmissionsschutzgesetzes ergibt sich nur eine Pflicht zur Erstellung der Überwachungspläne bzw. Überwachungsprogramme der zuständigen Behörden. Nach § 10 Abs. 1 des Thüringer Umweltinformationsgesetzes (ThürUIG) ergreifen die informationspflichtigen Stellen die notwendigen Maßnahmen, um in angemessenem Umfang eine aktive und systematische Verbreitung von Umweltinformationen in der Öffentlichkeit zu fördern. Nach Einschätzung des TLfDI kann § 10 Abs. 2 Nr. 2 ThürUIG nicht als Rechtsgrundlage für die Veröffentlichung personenbezogener Daten herangezogen werden. Nach dieser Vorschrift sind politische Konzepte sowie Pläne und Programme mit Bezug zur Umwelt zu veröffentlichen. Eine Veröffentlichungspflicht unter Nennung der betroffenen Anlagenbetreiber der jeweils zuständigen Behörden ergibt sich hieraus aber nicht. Das damalige Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) bestätigte auf Nachfrage des TLfDI, dass bei der Veröffentlichung von Überwachungsprogrammen personenbezogene Daten nicht veröffentlicht werden dürfen. Das Ministerium hatte aufgrund der Anfrage des TLfDI eine Kontrolle des im Internet veröffentlichten Überwachungsplans des Freistaats Thüringen veranlasst. Die Kontrolle hatte ergeben, dass in geringem

Umfang trotz aller Prüfung auch personenbezogene Daten in der Anlagenliste enthalten waren. Das TMLFUN hatte die Herausnahme von personenbezogenen Daten aus der Liste veranlasst, alle zuständigen Behörden auf die Rechtslage hingewiesen und zu einer Anonymisierung von personenbezogenen Daten vor der Veröffentlichung aufgefordert. Der TLfDI hat sich damit einverstanden erklärt, dass die Anlagenbetreiber in anonymisierter Form, also auch ohne die Vergabe von eindeutigen Kürzeln oder Initialen der Betroffenen im Überwachungsplan aufgenommen werden.

Überwachungsberichte nach dem Bundesimmissionsschutzgesetz, die im Internet nach den Thüringer Vorschriften veröffentlicht werden müssen, dürfen keine personenbezogenen Daten zum Betreiber der Anlage, zu seinen Mitarbeitern und zu weiteren Dritten enthalten.

12.6 Grundstücksgrenzen sind auch personenbezogene Daten

Ein Grundstückseigentümer beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass der zuständige Katasterbereich ihm keine Einsicht in die vollständigen, zu seinem Grundstück gespeicherten Daten gewährte. Darüber hinaus führte der Beschwerdeführer aus, dass die im Liegenschaftskataster eingetragenen Grundstücksgrenzen seines Grundstücks falsch seien. Der TLfDI teilte dem Beschwerdeführer zunächst mit, dass nach § 13 Thüringer Datenschutzgesetz (ThürDSG) die Daten verarbeitende Stelle dem Betroffenen auf Antrag Auskunft und Akteneinsicht über die zu seiner Person gespeicherten Daten zu erteilen habe und unrichtige personenbezogene Daten gemäß § 14 ThürDSG zu berichtigen seien. Unter Umständen habe der Betroffene darüber hinaus nach § 15 bzw. § 16 ThürDSG einen Anspruch auf Löschung von unrichtigen personenbezogenen Daten oder zumindest auf Sperrung der Daten, wenn ihre Richtigkeit vom Betroffenen bestritten werde. Allerdings wurde der Beschwerdeführer darauf aufmerksam gemacht, dass der TLfDI nicht berechtigt ist, die rein fachliche Arbeit einer Behörde zu überprüfen. Diesbezüglich wurde dem Bürger geraten, sich an die für die Katasterbereiche zuständige Aufsichtsbehörde, das Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo), zu wenden. Auf Bitte des Beschwerdeführers erfolgte ein persönliches Gespräch

beim TLfDI zum Sachverhalt, in dessen Verlauf dieser dem TLfDI mehrere Kopien von Unterlagen aus dem Liegenschaftskataster vorlegte, aus denen erkennbar sei, dass die Grenzen des betroffenen Grundstücks im Laufe der Jahre ohne erkennbaren Grund mehrfach geändert worden sein sollen. Außerdem sei die zu seinem Grundstück bestehende maßgebliche Liegenschaftskarte verfälscht worden, indem mehrere Längenmaße durch neue Maßangaben ersetzt worden sein sollen. Der TLfDI bat daraufhin die zuständige Katasterbehörde um Aufklärung des Sachverhalts. Eine Antwort erhielt der TLfDI aus dem TLVermGeo als obere Kataster- und Vermessungsbehörde, dem der Vorgang bereits bekannt war. Zunächst wurde die Auffassung des TLfDI nicht geteilt, dass es sich bei Grundstücksdaten, wie Größe und Grenzlängen um personenbezogene Daten handele. Der TLfDI verwies das Landesamt auf § 3 Abs. 1 ThürDSG, wonach alle Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person personenbezogene Daten sind. Da auch bei Grundstücksdaten ein Bezug zum betroffenen Grundstückseigentümer gegeben ist, sind dies personenbezogene Daten. Zum konkreten Sachverhalt führte das TLVermGeo gegenüber dem TLfDI aus, dass ein öffentlich bestellter Vermessungsingenieur eine erneute Vermessung der Grundstücksgrenzen vorgenommen und dabei festgestellt hätte, dass eine über 40 Jahre alte Vermessung des Grundstücks fehlerhaft gewesen sei. Im Ergebnis dieser Vermessung wurden einige Grenzmarken des Grundstücks zuungunsten des Beschwerdeführers verändert. Die Messergebnisse wurden dann dem betroffenen Grundstückseigentümer mit Bescheid bekannt gegeben. Wie sich durch Nachfrage des TLfDI beim Beschwerdeführer bestätigte, war der Bescheid bestandskräftig geworden. Da der Beschwerdeführer sich aber nach wie vor gegenüber dem TLfDI dahingehend äußerte, dass die aktuell durchgeführte Vermessung seiner Grundstücksgrenzen fehlerhaft gewesen sei, bat der TLfDI um ein gemeinsames Gespräch mit dem Beschwerdeführer, dem TLVermGeo und dem Katasterbereich, zu dem diese sich auch bereit erklärt hatten und bei dem auch die entsprechenden Katasterunterlagen vorgelegt werden sollten. Zur Abstimmung des Gesprächstermins wurde der Beschwerdeführer um Terminvorschläge gebeten.
Dafür schrieb ihn der TLfDI zwei Mal an, erhielt aber in beiden Fällen keine Antwort vom Beschwerdeführer. Deshalb konnte der TLfDI in diesem Fall leider nicht weiter tätig werden.

Grundstücksdaten über eine bestimmte oder bestimmbare Person sind personenbezogene Daten. Der Katasterbereich hat deshalb dem Betroffenen Auskunft über die dort zu seiner Person verarbeiteten Daten zu erteilen und ihm Einsicht in die ihn betreffenden Unterlagen zu gewähren. Grundsätzlich hat die öffentliche Stelle unrichtige Daten gemäß § 14 ThürDSG zu berichtigen, unzulässig gespeicherte Daten gemäß § 16 Abs. 1 Nr. 1 ThürDSG zu löschen und Daten, bei denen sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, gemäß § 15 Abs. 1 Nr. 1 ThürDSG zu sperren. Wenn ein Bescheid über eine Grundstücksvermessung durch einen öffentlich bestellten Vermessungsingenieur bestandskräftig wird, kann die verantwortliche Stelle davon ausgehen, dass die im Liegenschaftskataster eingetragenen Grundstücksdaten den Tatsachen entsprechen.

12.7 Thüringen in 3-D

Die Daten des amtlichen Vermessungswesens (z. B. Gebäude, Grundstücke, Straßen, Landschaftsbeschaffenheit usw.) werden als Geobasisdaten bezeichnet und müssen vom amtlichen Vermessungswesen beschrieben und nachgewiesen werden. Bisher erfolgte die Bereitstellung der Geobasisdaten seitens der Katasterverwaltung in zweidimensionaler Darstellung. Zur Einführung der Darstellung von dreidimensionalen Geobasisdaten, die jedermann ohne Zugangsbeschränkung über den Geoclient des Geoproxy (http://www.geoproxy.geoportal-th.de/geoclient/start_geoproxy.jsp) verfügbar gemacht werden, wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfD) um eine datenschutzrechtliche Stellungnahme gebeten. Der TLfDI nahm hierzu an einer Beratung im Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo) teil, in der das um die dritte Dimension erweitere Verfahren vorgestellt wurde. Nach Ausführung des TLVermGeo werden die Gebäudemodelle in einer ersten Stufe derzeit als einfaches Klötzchenmodell (so genannte LoD 1=Level of Detail Stufe 1) dargestellt. Mittelfristig ist dann die Einführung eines dreidimensionalen Gebäudemodells mit standardisierten Dachformen geplant (LoD 2), das dann ebenfalls in Geoproxy zur Verfügung

gestellt werden soll. Die Gebäude- und Landschaftshöhen werden mithilfe eines Laserscannings mittels Befliegen ermittelt. Nach Auffassung des TLVermGeo erfülle der Freistaat Thüringen mit der Bereitstellung des Zugangs zu den Geobasisdaten die Forderungen der EU-Richtlinie „INSPIRE“, die den Rahmen für eine gemeinsame Geodateninfrastruktur in Europa vorgibt. Nach Prüfung des vorgetragenen Sachverhalts, der vorgeführten dreidimensionalen Beispielbilder von Gebäudemodellen mit standardisierten Dachformen sowie unter Berücksichtigung der hierzu bestehenden Rechtsvorschriften, insbesondere von § 5 Abs. 1 des Thüringer Geodateninfrastrukturgesetzes, wonach Geodaten, Metadaten und Geodatendienste *„… öffentlich verfügbar und über das Internet … zugänglich sein*“ müssen, hat der TLfDI keine datenschutzrechtlichen Bedenken gegen die Einführung solcher dreidimensionalen Darstellungen von Geobasisdaten geltend gemacht.

Die öffentliche Verfügbarmachung von Geobasisdaten für jedermann ist in Thüringen wie auch in den anderen Bundesländern erlaubt. Hiermit werden die Forderungen der EU-Verordnung „INSPIRE“ umgesetzt. Der Detaillierungsgrad der Geobasisdaten wird weiter voranschreiten. Der TLfDI wird diese Entwicklung verfolgen.

12.8 Videoüberwachung im ÖPNV – Videogaga 4

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom damaligen Thüringer Ministerium für Bau, Landesentwicklung und Verkehr (TMBLV) um Beratung gebeten, welche Rechtsvorschriften bei der Förderung von Videoüberwachungsanlagen in Bussen, Straßenbahnen, Zügen, auf dem Busbahnhof oder Bahnhof sowie bei der Ausschreibung von Verkehrsleistungen im Schienenpersonennahverkehr zu beachten sind. Der TLfDI legte dem Ministerium dar, dass für die Datenschutzaufsichtsbehörde immer die verantwortliche Stelle Ansprechpartner ist. Dies sind die Unternehmen oder Stellen, die die Videoüberwachungsanlage betreiben. Diese sind nach dem Gesetz verpflichtet, die geltenden Datenschutzbestimmungen einzuhalten. Eine Einwilligung kommt bei einer Videoüberwachung nicht in Betracht, da die gesetzlichen Voraussetzungen hierfür nicht eingehalten werden können, etwa hinsichtlich der Freiwilligkeit, der schriftlichen Einwilligung, der umfassenden Aufklärung über die Maßnahme etc.

Eine Videoüberwachung ist daher nur zulässig, wenn eine Rechtsvorschrift sie ausdrücklich erlaubt. In Betracht kommt hier in erster Linie die Bestimmung des § 6b Bundesdatenschutzgesetz. Die Videoüberwachung ist danach nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach Auffassung des TLfDI ist nach dem geltenden Recht jedenfalls eine flächendeckende Videoüberwachung in Fahrzeugen des ÖPNV unzulässig. Dem TMBLV wurde empfohlen, im Rahmen der Ausschreibung von Förderungen den verantwortlichen Stellen keine detaillierten Vorgaben für eine ausnahmslose Videoüberwachung zu machen, da deren Zulässigkeit immer nur anhand der Umstände des Einzelfalls beurteilt werden kann. In jedem Fall sind der Umstand einer Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen, im Regelfall durch gut sichtbar angebrachte Schilder, erkennbar zu machen. Der TLfDI hatte das TMBLV auch darüber informiert, dass in aller Regel die verantwortliche Stelle, die eine Videoüberwachung mittels digitaler Aufzeichnung durchführt, einen Beauftragten für den Datenschutz zu bestellen hat. Dieser hat vor Inbetriebnahme der Videoüberwachungsanlage eine so genannte Vorabkontrolle durchzuführen. Zusätzlich wurde das Ministerium auf die Empfehlung „Videoüberwachung in öffentlichen Verkehrsmitteln“ sowie auf die Orientierungshilfe „Videoüberwachung“ (siehe Nummer 2.6) des Düsseldorfer Kreises verwiesen. Inzwischen wurde die Empfehlung „Videoüberwachung in öffentlichen Verkehrsmitteln durch die Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ mit Stand 16. September 2015 ersetzt. Sämtliche Papiere wurden dem TMBLV bzw. dem jetzt zuständigen Thüringer Ministerium für Infrastruktur und Landwirtschaft zur Kenntnis gegeben. Die Dokumente sind auch auf der Homepage des TLfDI unter https://www.tlfdi.de/tlfdi/themen/orientierungshilfen veröffentlicht worden.

Da eine Erforderlichkeit des Einsatzes von Videoüberwachung im ÖPNV von zahlreichen Faktoren bestimmt wird und nur anhand der

Umstände im Einzelfall beurteilt werden kann, sollten in einem öffentlichen Ausschreibungstext den verantwortlichen Stellen keine detaillierten Vorgaben zur ausnahmslosen Videoüberwachung gemacht werden.

12.9 PKW-Maut ohne flächendeckende Datenerhebung

Ein Landesdatenschutzbeauftragter bat seine Bundes- und Landeskollegen und -kolleginnen um Stellungnahme zur geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen. Die Bundesregierung schlug als Verfahren eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer an flächendeckend installierten elektronischen Kontrollpunkten vor. Der genannte Entschließungsentwurf forderte von der Bundesregierung, auf die Einrichtung eines solchen elektronischen Verfahrens, mit dem hunderttausende Kfz-Kennzeichnen erfasst werden würden, zu verzichten. Zum einen widerspricht diese Verfahrensweise den verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und der Datensparsamkeit, zum anderen ist die Maßnahme zur Mauterhebung nicht erforderlich. Für Abrechnungs- und Kontrollzwecke des Staates stehen z. B. mit der Einführung einer Vignette nach dem Vorbild anderer Staaten mildere und ebenso effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seiner Stellungnahme den Entschließungsentwurf mitgetragen und insbesondere die Vignettenlösung bevorzugt, da hierbei nur ein geringer Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen erfolgt. Gleichzeitig brachte der TLfDI zum Ausdruck, andere Lösungen, mit denen Kfz-Kennzeichen oder sogar ein Bild der Fahrzeuge erhoben, verarbeitet und genutzt werden, in der Entschließung grundsätzlich nicht anzusprechen, da unabhängig davon, wie ein solches Verfahren technisch gestaltet ist, bei den Sicherheitsbehörden Begehrlichkeiten geweckt würden, die mit der Vignettenlösung von vornherein vermieden werden könnten. Der TLfDI erinnerte dabei an die Probleme von Zweckerweiterungen der Fotoaufnahmen der Fahrzeuge im Zusammenhang mit der damaligen Einführung der LKW-Maut. In Auswertung der Stellungnahme aller Datenschutzbeauftragten des Bundes und der Länder wurde in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

mit Datum vom 14. November 2014 die Entschließung „Keine PKW-Maut auf Kosten des Datenschutzes!“ verabschiedet und vom TLfDI in einer Pressemitteilung veröffentlicht (siehe dazu Anlage 42).

Bei der Einführung einer PKW-Maut ist aus datenschutzrechtlicher Sicht die Vignetten-Lösung zu bevorzugen. Der Eingriff in das Recht auf informationelle Selbstbestimmung ist hierbei gering. Gleichzeitig hat sich die Vignette bei der Erhebung von Mautgebühren in anderen Ländern bewährt.

12.10 Amtshilfe wegen MPU-Gutachten

Ein behördlicher Datenschutzbeauftragter einer Kommune setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass die Steuerfahndungsstelle eines Finanzamtes im Rahmen der Amtshilfe von Fahrerlaubnisbehörden personenbezogene Daten zu Gutachten zur Fahrtüchtigkeit fordere. Im Einzelnen sollten der Name, die Anschrift, das Geburtsdatum der Begutachteten genannt sowie die Daten der jeweiligen Gutachten in „geeigneter Weise“ belegt werden.
Als Rechtsgrundlage für das Amtshilfeersuchen verwies das Finanzamt auf § 111 Abgabenordnung (AO), der in seinem Abs. 5 auch § 105 AO für entsprechend anwendbar erklärt. Diese Vorschrift greift dann ein, wenn die ersuchte Behörde durch die Amtshilfe ihre Verschwiegenheitspflicht verletzen würde. Die o. g. Daten dürfen nach § 2 Abs. 9 Satz 1 Straßenverkehrsgesetz ausschließlich zur Feststellung oder Überprüfung der Eignung oder Befähigung zur Fahrtüchtigkeit verwendet werden. Zudem enthalten Gutachten zu Fahrtüchtigkeit in der Regel hochsensible Sozialdaten, die dem Sozialgeheimnis nach § 35 Sozialgesetzbuch I unterliegen.
Auf die Anfrage des TLfDI teile das Finanzamt u. a. mit, dass die Daten Name, Vorname und Geburtsdatum der Begutachteten und das Datum des Gutachtens für Vorermittlungen im Besteuerungsverfahren erforderlich seien. Hierbei gehe es insbesondere darum, die zu begutachtenden Personen eindeutig zu identifizieren und den Zeitraum der Rechnungslegung des Gutachters einzugrenzen. Demgegenüber sei der Inhalt der Gutachten nicht erforderlich, weshalb sie nicht vorzulegen seien.

Da die Formulierung in den Amtshilfeersuchen, dass neben den o. g. konkret bezeichneten personenbezogenen Daten auch die Daten der jeweiligen Gutachten „in geeigneter Weise“ zu belegen seien, bei den Fahrerlaubnisbehörden zu Irritationen führte, forderte der TLfDI das Finanzamt auf, dafür Sorge zu tragen, dass künftig gegenüber den ersuchten Stellen nur die im Besteuerungsverfahren benötigten, konkret bezeichneten Daten angefordert werden. Dies würde die in datenschutzrechtlicher Hinsicht gebotene Transparenz des Verfahrens erhöhen und ausschließen, dass für die Aufgabenerledigung nicht benötigte sensible personenbezogene Daten in unzulässiger Weise übermittelt werden.
Das Finanzamt erklärte daraufhin gegenüber dem TLfDI, dass die Verwendung der Formulierung „in geeigneter Weise“ im konkreten Fall des Steuerfahndungsverfahrens die Gefahr von Unklarheiten barg. Daher seien die Mitarbeiter der Steuerfahndungsstelle entsprechend sensibilisiert und im Sinne des Hinweises des TLfDI belehrt worden. Überdies sei das zuständige Fachreferat der Thüringer Landesfinanzdirektion hiervon in Kenntnis gesetzt worden.

Eindeutige Formulierungen hinsichtlich der benötigten personenbezogenen Daten sind sowohl in Amtshilfeersuchen, in Formularen zur Datenerhebung als auch in der Software zur Dateneingabe unabdingbar. Dadurch können das datenschutzrechtliche Transparenzgebot garantiert und unzulässige Datenerfassungen bzw. -übermittlungen sowie etwaige Irritationen bei „Datenlieferanten“ vermieden werden.

12.11 Das Wageninnere: von Interesse auch für die Ordnungskräfte

Aus dem Rundschreiben eines anderen Landesdatenschutzbeauftragten hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfahren, dass im dortigen Bundesland in einigen Kommunen die für die Parkraumüberwachung eingesetzten kommunalen Mitarbeiterinnen und Mitarbeiter Parkverstöße mittels Digitalaufnahmen dokumentieren. Wenn der Parkschein oder die Parkscheibe offensichtlich fehlte, wurde darüber hinaus das gesamte Wageninnere fotografiert. Nach Angaben der angefragten Ordnungsbehörde könne man mit diesen Fotobeweisen besser Behauptungen entgegentreten, der Parkschein bzw. die Parkscheibe sei ins Wageninnere gefallen. Nach Auffassung des TLfDI ist eine sol-

che Verfahrensweise aus datenschutzrechtlichen Gründen völlig inakzeptabel. Gemäß § 13 Abs. 1 Satz 1 der Straßenverkehrsordnung (StVO) muss der Parkschein am oder im Fahrzeug von außen gut lesbar angebracht sein, Gleiches gilt nach § 13 Abs. 2 Nr. 2 StVO auch für die Parkscheibe. Als gut lesbare Orte kommen im Fahrzeug grundsätzlich nur das Armaturenbrett und die Front-, Seiten- oder Heckscheiben (da einige Parkscheiben Saugnäpfe haben), eventuell auch noch die so genannte Hutablage oder bei Kombis die Kofferraumabdeckung infrage. Falls eine Ordnungsbehörde tatsächlich meint, einen ausführlichen Fotobeweis des gesamten einsehbaren Innenraums eines Fahrzeugs anfertigen zu müssen, ist dies aus datenschutzrechtlicher Sicht unzulässig. Für den Nachweis, dass ein Parkschein oder die Parkuhr eben nicht von außen gut lesbar angebracht war, ist das Fotografieren in das Innere des Autos und damit die Dokumentation, wie es darin ausgesehen hat, für die Aufgabenerfüllung nicht erforderlich, § 19 Abs. 1 Thüringer Datenschutzgesetz. Falls ein Parkschein oder eine Parkscheibe ins (nicht gut einsehbare) Autoinnere gefallen ist, geht dies nach Ansicht des TLfDI zulasten des Fahrzeughalters. Darüber hinaus sind die Ordnungsamtsmitarbeiter, die die schriftliche Verwarnung ausstellen, auch ohne Fotobeweis gleichzeitig Zeugen hinsichtlich des fehlenden Parkscheins bzw. der Parkscheibe. Der TLfDI kann sich weder vorstellen, dass die Zahl der Einsprüche mit der in Rede stehenden Begründung, wonach der Parkschein ins Innere gefallen sei, hoch ist, noch dass ein entsprechendes Gericht einer solchen Einlassung eines Kfz-Halters folgen wird. Der TLfDI geht davon aus, dass die Ordnungskräfte in Thüringen die Fahrzeuginnenräume in den dargelegten Fällen nicht fotografisch zu Beweiszwecken dokumentieren. Zumindest sind keine diesbezüglichen Beschwerden laut geworden.

Soweit eine Erforderlichkeit hierfür besteht, dürfen Ordnungsbehörden mittels eines Kamerabeweises einen Parkverstoß dokumentieren. Das Abfotografieren des Innenraums ist hiervon keinesfalls erfasst und deshalb unzulässig.

12.12 Im Tower alles im Blick – Videogaga 5 – Videoüberwachung am Flughafen

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit TLfDI) kontrollierte im Berichtszeitraum die

Videoüberwachung an einem Flughafen in Thüringen. Naturgemäß gab es an dem Flughafen einige Kameras. Ein Flughafen besitzt auch immer ein hohes Sicherheitsrisiko, dem auch mit dem Einsatz von Videoüberwachung begegnet werden soll. Die Kameras, die von der Bundespolizei eingesetzt und auch nur von dieser eingesehen werden können, unterliegen nicht der Kontrolle des TLfDI. Er prüfte die Zulässigkeit der Kameras, die im Parkhaus und auf dem Flughafengelände von dem Betreiber des Flughafens genutzt wurden. Auf den Flughafen ist das Bundesdatenschutzgesetz (BDSG) anwendbar. Zwar handelt es sich nach § 2 Absatz 2 Thüringer Datenschutzgesetz (ThürDSG) um eine öffentliche Stelle. Allerdings bestimmt § 26 ThürDSG, dass, soweit öffentliche Stellen am Wettbewerb teilnehmen, auf sie von den Bestimmungen des ThürDSG nur der 5. Abschnitt, ausgenommen § 34 Abs. 2, anzuwenden ist, im Übrigen gelten für sie die Bestimmungen des BDSG mit Ausnahme des 2. Abschnitts und des § 38. Die Flughäfen stehen, zumindest soweit sie sich in räumlicher Nähe befinden, untereinander im Wettbewerb im Hinblick auf die potenziellen Fluggäste.

Wie es bei dem Einsatz einer Vielzahl von Kameras erforderlich ist, gab es für den Flughafen einen Datenschutzbeauftragten, der auch die nach § 4d Abs. 5 BDSG erforderliche Vorabkontrolle durchgeführt hatte. Ziel dieser technisch-organisatorischen Analyse ist die Bewertung der Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung. Geprüft werden muss dabei, ob der geplante Einsatz jeder einzelnen Kamera jeweils den gesetzlichen Anforderungen entspricht und welche technischen und organisatorischen Maßnahmen zu ihrer Einhaltung zu ergreifen sind. Lassen sich erkannte Restrisiken nicht hinreichend sicher ausgestalten, darf ein Verfahren so nicht zum produktiven Einsatz kommen. Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte. Die Zulässigkeit der Videoüberwachung beurteilte sich nach § 6b Absatz 1 BDSG. Danach ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen.

Zunächst fiel dem TLfDI auf, dass die Speicherdauer der Aufzeichnungen mit einer Woche zu lang war. Gemäß § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen,

wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht mehr notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können, da der Flughafen 24 Stunden an sieben Tagen in der Woche geöffnet ist. Das bedeutet, dass Videoaufzeichnungen grundsätzlich nach 48 Stunden zu löschen sind (vgl. Gesetzesbegründung, Bundestagsdrucksache 14/5790, Seite 63). Für einen Großteil der Kameras wurde daher eine Speicherdauer von maximal 48 Stunden als ausreichend angesehen. Etwas anderes galt für die Kameras, die sich im Schrankenbereich des Parkhauses sowie der Parkplätze befinden. Der Betreiber des Flughafens hatte glaubhaft dargelegt, dass es zahlreiche Urlauber gibt, die den Parkplatz für einen längeren Zeitraum nutzen und es bei Verlust des Parkscheines häufiger zu Problemen wegen der Nichtbeweisbarkeit der Standdauer des PKW komme. Für die Einfahrt in die Parkgarage bzw. auf den Parkplatz wurde daher eine längere Speicherdauer für zulässig erachtet.
Alle für die jeweiligen Kameras angegebenen Zwecke wurden geprüft. Jede einzelne Kamera muss tatsächlich für den festgelegten Zweck geeignet und erforderlich sein. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel, erreicht werden kann. Nicht alle angegebenen Zwecke rechtfertigten eine Videoaufzeichnung. In einigen Bereichen sollte die Videoaufzeichnung Zugänge sichern und die Zufahrt für Not- und Rettungseinsätze sichern. Für diese Zwecke würde es ausreichen, wenn ein reines Monitoring, also die Beobachtung der Liveaufnahmen, stattfindet. In der Vorabkontrolle war angeführt, dass eine permanente Überwachung der Mitarbeiter nicht stattfindet, und außerdem wurde bei den jeweiligen Kameras mit angegeben, welche Personen Einsicht nehmen dürfen. Es fehlte jedoch eine schriftliche Festlegung, unter welchen Voraussetzungen überhaupt Zugriff auf die Videoaufzeichnungen genommen werden darf. In diesen Punkten hat der TLfDI Nachbesserung gefordert. Das Verfahren ist noch nicht abgeschlossen.

Auch wenn auf einem Flughafen ein erhöhtes Sicherheitsrisiko besteht, darf eine Videoüberwachung nur stattfinden, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen, § 6b BDSG. Die Speicherdauer von Videoaufzeichnungen kann in einem Flughafenparkhaus länger sein, weil es dort viele über einen längeren Zeitraum parkende Nutzer gibt.

12.13 Video im Bus – kein Muss – Videogaga 6

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine anonyme Anzeige gegen ein Busunternehmen in Thüringen ein. Der Eigentümer des Unternehmens habe kürzlich neue Fahrzeuge angeschafft und in diesen Videotechnik installiert. Dabei werde das komplette Innere des Busses einschließlich des Sitzes des Busfahrers selbst überwacht. Außerdem werde auch noch ein Teil des Straßenbereichs vor dem Bus aufgenommen. Der TLfDI stattete dem Busunternehmen einen Besuch ab und kontrollierte dort die vom Unternehmen durchgeführte Videoüberwachung. Dabei stellte sich heraus, dass zur Objektsicherung des Betriebsgeländes 14 Kameras zum Einsatz kamen. Die in der anonymen Anzeige gemachten Angaben bestätigten sich vor Ort. Die modernen Busse des Unternehmens waren mit einer Videoüberwachung ausgestattet, die sowohl die Fahrgäste als auch den Busfahrer überwachte. Auch ein Teil des Straßenbereichs vor dem Bus wurde mit aufgezeichnet. Der Inhaber des Unternehmens teilte mit, dass er hinsichtlich der Überwachung in den Bussen davon ausgegangen sei, dass diese unproblematisch sei, da die Fahrzeuge mit der entsprechenden Ausstattung angeboten worden seien und die Ausrüstung der Fahrzeuge auch durch ein Förderprogramm des Freistaates Thüringen mit 75 Prozent der Anschaffungskosten gefördert worden sei.
Im Rahmen des Arbeitskreises Verkehr erfuhr der TLfDI zwischenzeitlich, dass die Videoüberwachungen in Bussen und sonstigen Unternehmen des öffentlichen Personennahverkehrs auch in anderen Ländern deutlich zugenommen hat. Auch die Aufsichtsbehörden der anderen Länder sahen das Bedürfnis, für diesen Bereich einheitliche Festlegungen zu treffen. Die Aufsichtsbehörden beschlossen daher,

eine Orientierungshilfe für die Videoüberwachung im öffentlichen Personennahverkehr zu erarbeiten (siehe Nummer 12.8).
Der TLfDI stellte das Verfahren der Prüfung der Videoüberwachung des Busunternehmens aus diesem Grund zunächst zurück, um das Ergebnis der Beratungen über die Orientierungshilfe abzuwarten. Nachdem die Orientierungshilfe vom Düsseldorfer Kreis beschlossen wurde, trat der TLfDI erneut an das Busunternehmen heran und bat dieses zunächst, die auf dem Betriebsgelände und in den Dienstbussen aktuell durchgeführte Videoüberwachung nochmals darzulegen. Es war nicht ausgeschlossen, dass sich aufgrund des Zeitablaufs zwischenzeitlich Änderungen ergeben hatten. Der TLfDI wird die durchgeführte Videoüberwachung anhand der Festlegungen der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ prüfen. Es ist davon auszugehen, dass eine lückenlose Überwachung des Busfahrers jedenfalls nicht zulässig sein wird, da nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz personenbezogene Daten eines Beschäftigten zur Aufdeckung von Strafdaten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Für das Unternehmen wird außerdem schwer zu begründen sein, warum der öffentliche Verkehrsraum mitüberwacht werden muss und eine nahezu lückenlose Überwachung der Busse durchgeführt wird. Das weitere Verfahren bleibt abzuwarten.

Auch im öffentlichen Personennahverkehr ist eine Videoüberwachung nicht grundsätzlich zulässig, sie muss im Rahmen geltender Datenschutzgesetze durchgeführt werden. Der TLfDI wird die in der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ festgelegten Grundsätze bei der Prüfung zugrunde legen.

12.14 Tunnelblick

Ende Oktober/Anfang November 2014 wurde der Jagdbergtunnel der Autobahn A 4 bei Jena eröffnet und für den Verkehr freigegeben. Aus diesem Anlass wandte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an das zuständige Landesamt für Bau und Verkehr Thüringen und bat um Auskunft über die in den Tunnelröhren eingesetzten Videokameras,

deren Anzahl und die Übertragung von Videobildern an öffentliche Stellen.
Das Landesamt Bau und Verkehr antwortete prompt und teilte mit, dass die Videodaten zur Gefahrenabwehr an die zentrale Betriebsleitstelle für alle Straßentunnel in Thüringen nach Zella-Mehlis übertragen würden. Daneben erfolge eine Übermittlung für alle Straßentunnel an die Autobahnpolizeiinspektion (API) in Schleifreisen und die Autobahnpolizeistation Süd in Zella-Mehlis, welche für die Tunnelkette Thüringer Wald zuständig sei. Auch an die Feuerwehr der Stadt Suhl und an die Feuerwehr der Stadt Jena finde eine Übertragung der Videodaten statt. Insgesamt seien 127 Kameras im Tunnel eingesetzt.
Daraufhin forderte der TLfDI das Thüringer Ministerium für Inneres und Kommunales (TMIK) auf, ihm die Rechtsgrundlage für eine Übermittlung der Videobilder aus dem Jagdbergtunnel an die API zu nennen.
Eine Rechtsgrundlage für die Übermittlung dieser Videobilder war aus der Sicht des TMIK nicht erforderlich. Das Ministerium begründete seine Rechtsauffassung unter Hinweis darauf, dass es sich bei den Videobildern um Übersichtsaufnahmen handele, auf denen weder Personen noch amtliche Kfz-Kennzeichen erkennbar seien. Deshalb würden keine personenbezogenen Daten mittels der Videobilder erhoben, sodass kein Grundrechtseingriff stattfinde und daher auch keine Rechtsgrundlage für die Übermittlung der Videobilder erforderlich sei.
Der TLfDI konnte sich mit dieser Antwort noch nicht zufriedengeben: Für ihn war es entscheidend, ob auf den erhobenen Videobildern aus dem Jagdbergtunnel tatsächlich keine personenbezogenen oder personenbeziehbaren Daten enthalten waren. Deshalb wollte er vom TMIK wissen, welche Auflösung die Videobilder besitzen, die mit den Kameras aus dem Jagdbergtunnel angefertigt werden. Ferner interessierte den TLfDI auch der Öffnungswinkel der im Jagdbergtunnel eingesetzten Kameras.
Die Antworten des TMIK auf diese datenschutzrechtlich relevanten Fragen lagen bis zum Redaktionsschluss für den 11. Tätigkeitsbericht noch nicht vor. Der TLfDI wird daher im nächsten Tätigkeitsbericht darüber informieren, welche Bilder in welcher Auflösung im Jagdbergtunnel erhoben werden.

Mit der Kfz-Kennzeichenerfassung in Thüringer Tunneln hat der TLfDI schon datenschutzrechtlich negative Erfahrungen gesammelt: Erinnert sei hier nur an die „automatische Kennzeichenerfassung“ im Rennsteigtunnel trotz fehlender Rechtsgrundlage (siehe dazu den 5. Tätigkeitsbericht, Nr. 7.5 – Automatische Gesichts- und Kennzeichenerfassung, Seite 86 f.). Deshalb ist bei einer Bild- oder Videoübermittlung aus einem Tunnel an die Polizei besonderes datenschutzrechtliches Augenmerk geboten: Erst wenn klar ist, dass tatsächlich keine personenbezogenen oder personenbeziehbaren Daten von den Kameras aus dem Jagdbergtunnel erhoben werden, bedarf es dafür auch keiner Rechtsgrundlage. Dies ergibt sich aus § 4 Abs. 1 Satz 1 ThürDSG und für die Polizei insbesondere aus § 31 Abs. 1 Polizeiaufgabengesetz. Ob im Jagdbergtunnel tatsächlich keine personenbezogenen Daten mittels Kamera erhoben werden, hat der TLfDI im Rahmen seiner Aufgaben gemäß § 37 Abs. 1 ThürDSG zu prüfen.

12.15 Erforschung der Energieeffizienz

Eine Universität wandte sich mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es war ein Forschungsprojekt „Energieeffizienz in der Stadt“ geplant. Ziel war, in einer bestimmten Modellregion ein Planungsinstrument zur Verfügung zu stellen, welches es ermöglichen sollte, Effizienzmaßnahmen in die kommunale Stadtentwicklung zu integrieren. Hierfür beabsichtigte die Universität, über die Bereitstellung von Kennzahlen eine hinreichende Abschätzung des Verbrauchs zu ermöglichen. Zur Erarbeitung dieser Kennzahlen wurden Geobasisdaten der Region zur Analyse und Visualisierung funktioneller Zusammenhänge sowie gebäudescharfe Energieverbrauchsdaten und die gebäudespezifische Einwohnerzahl ohne Nennung der Namen benötigt. Außerdem wurde zur notwendigen Ermittlung der anfallenden Abwassermengen der Wasserverbrauch pro Gebäude benötigt. Die aus diesen Daten zu generierenden gebäudespezifischen Kennzahlen sollten lediglich über statistische Angaben wie die Gesamtheit gleicher Gebäudetypen, bestimmte Baublöcke (ein von vier Straßen umgebenes Quartier) oder noch größer über Stadträume (mehrere Blöcke gleichen Typs) veröffentlicht werden. Die Universität hatte alle am Projekt Beteiligten im Hinblick auf den Datenschutz geschult, und sie waren auf das Datengeheimnis ver-

pflichtet worden. Die Daten sollten auf einem separaten, nur dafür vorgesehenen Rechner ohne Zugriff auf das Internet verarbeitet werden. Die Festplatte sollte zudem verschlüsselt werden.
Der TLfDI teilte der Universität mit, dass das Erheben personenbezogener Daten zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist, § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden, § 25 Abs. 1 ThürDSG. Nach § 25 Abs. 3 ThürDSG sind die personenbezogenen Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Die Universität hatte nachvollziehbar dargelegt, aus welchen Gründen die zu erhebenden Daten nicht in anonymisierter Form ausreichen. Allerdings hat sie sicherzustellen, dass die gespeicherten personenbezogenen Daten entsprechend den Vorgaben des § 25 Abs. 1 ThürDSG nur für die verfolgten Forschungszwecke verwandt und die gewonnenen Erkenntnisse in anonymisierter Form dargestellt werden. Die Mitglieder der Forschungsgruppe sind darauf hinzuweisen, dass eine Weitergabe der personenbezogenen Daten an Dritte nicht zulässig ist.
Problematischer gestaltete sich die Übermittlungsbefugnis der Stellen, bei denen die benötigten Daten vorhanden sind, beispielsweise Einwohnermeldeämter der betroffenen Kommunen und Energieversorger.
Der TLfDI ging davon aus, dass die Universität die Geobasisdaten der betroffenen Gemeinden über den Geoproxyserver des Thüringer Landesamtes für Vermessung und Geoinformation erhalten würde, insoweit bestanden keine datenschutzrechtlichen Bedenken. Auch Geobasisdaten stellen personenbezogene Daten dar, da sie sich immer auf ein Grundstück beziehen und damit Rückschlüsse auf den Eigentümer des Grundstücks zulassen. Nach § 5 Abs. 1 des Thüringer Geodateninfrastrukturgesetzes müssen Geodaten öffentlich verfügbar und über das Internet und andere geeignete Kommunikationsmittel zugänglich sein.
Für die Übermittlung der gebäudescharfen Energieverbrauchsdaten als Sachdaten sowie der Einwohnerzahl für die jeweiligen Adressen gab es keine spezielle Ermächtigungsgrundlage, daher galten die allgemeinen Bestimmungen des ThürDSG. Da die Universität eine öffentliche Stelle im Sinne von § 2 Abs. 1 ThürDSG ist, gilt für die

Datenübermittlung durch die Kommune § 21 ThürDSG. Fraglich ist, ob die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Danach muss die Übermittlung für Zwecke erfolgen, für die die Daten bei der Daten erhebenden Stelle erhoben worden sind. Dies war nicht der Fall, da die Daten ursprünglich nicht für die Übermittlung an die Universität erhoben wurden, sondern für andere Zwecke. Eine Übermittlung für andere Zwecke ist nur unter den Voraussetzungen des § 20 Abs. 2 ThürDSG zulässig. In Betracht kam hier § 20 Abs. 2 Nr. 9 ThürDSG. Danach muss die Übermittlung dann zur Durchführung von wissenschaftlicher Forschung erforderlich sein, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens muss das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegen und der Zweck der Forschung muss auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können. Die Erforderlichkeit der Daten für die wissenschaftliche Forschung lag auf der Hand und es bestand auch kein Zweifel daran, dass der Zweck der Forschung auf andere Weise nicht bzw. nur mit unverhältnismäßigem Aufwand erreicht werden konnte. Fraglich war, ob das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt. Bei den Daten zum Strom-, zum Wasserverbrauch sowie zum Abfall- und Abwasseranfall handelt es sich um personenbezogene Daten, die Auskunft über das Verbrauchsverhalten der Personen geben, die unter einer Adresse gemeldet sind. Die Namen der Einwohner werden nicht genannt, nur die Zahl der Einwohner, die unter einer bestimmten Adresse gemeldet sind. Eine eindeutige Zuordnung des Verbrauchsverhaltens ist daher nur in den Fällen möglich, in denen unter einer bestimmten Adresse nur eine Person gemeldet ist. In allen anderen Fällen ist die Zuordnung umso mehr erschwert, je mehr Personen unter einer Adresse gemeldet sind. Unter folgenden Voraussetzungen erschien die Übermittlung der Daten dem TLfDI noch als von § 20 Abs. 2 Nr. 9 ThürDSG gedeckt:

Es muss sich um eine einmalige Datenlieferung zu einem bestimmten Zeitraum für ein abgegrenztes Gebiet (beispielsweise das Gebiet einer Gemeinde) handeln. Es werden keine Einwohnernamen erhoben, sondern die Daten lediglich zu den Adressen zugeordnet. Zugriff auf diese Daten haben nur die Mitglieder der Forschungsgruppe, wobei diese auf das Datengeheimnis nach § 6 ThürDSG zu ver-

pflichten sind. Die Forschungsergebnisse dürfen keine Rückschlüsse auf den Energieverbrauch bestimmter Personen oder Adressen zulassen. Die statistisch aufbereiteten Daten sollen immer nur aggregiert für eine gewisse Anzahl von Adressen übermittelt werden. Die Daten müssen auf dem Server der Universität in einem gesonderten Mandanten vorgehalten werden, zu dem nur die Mitglieder der Forschungsgruppe Zugang haben. Die Festplatte ist zu verschlüsseln. Nach Ablauf des Projekts müssen die Daten gelöscht werden, sobald sie zu Forschungszwecken nicht mehr benötigt werden.
Nachdem den Forschern die Einhaltung der datenschutzrechtlichen Anforderungen von hoher Bedeutung war, geht der TLfDI davon aus, dass die Anforderungen umgesetzt werden. Eine datenschutzrechtliche Prüfung behält der TLfDI sich vor.

Weil die Forschung mit personenbezogenen Daten oftmals unerlässlich ist, um einen bestimmten Forschungszweck zu erreichen, sieht das ThürDSG ein so genanntes Forschungsprivileg vor. Nach § 20 Abs. 2 Nr. 9 ThürDSG ist die Übermittlung von personenbezogenen Daten an öffentliche Forschungseinrichtungen zulässig, wenn sie zur Durchführung von wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

12.16 Wolf unter Beobachtung – zu Wildkameras

Das Thüringer Ministerium für Umwelt, Energie und Naturschutz (TMUEN) wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um datenschutzrechtliche Beurteilung einer geplanten Videoüberwachung durch so genannte Wildkameras zur Wolfsbeobachtung in einem bestimmten Thüringer Waldgebiet, in dem der Wolf bereits gesichtet worden war.
Die Videoüberwachung sei zur Beobachtung der vermuteten und nachgewiesenen Aufenthaltsorte und Laufwege aus wissenschaftlichen Zwecken erforderlich und für die wissenschaftliche Auswertung unverzichtbar. Insbesondere die Fauna, Flora, Habitat (FFH)-Richtlinie (Richtlinie 92/43/EWG) und § 6 in Verbindung mit

§ 7 Abs. 2 Nr. 14 des Bundesnaturschutzgesetzes (BNatSchG) verpflichte das Land, über den Haltungszustand durch Beobachtung zu berichten. In Bezug auf wildlebende Wölfe sind alle erforderlichen Maßnahmen zu treffen, um die natürlichen Lebensräume und die Population zu erhalten oder diese wiederherzustellen. Gemäß Artikel 11 der FFH-Richtlinie sind die Mitgliedstaaten zur Überwachung des Erhaltungszustandes der Arten verpflichtet, die eine Beobachtung auch der Wölfe voraussetzt. Die Durchführung ist in § 6 BNatSchG niedergelegt. Das Thüringer Ministerium für Umwelt, Energie und Naturschutz (TMUEN) hatte hierzu die Installation von 10 Wildkameras vorgesehen.

Die Problematik ist äußerst vielschichtig, da die Verantwortlichkeit für die Videoüberwachung in einem Waldgebiet mit unterschiedlichen Eigentümern teils beim TMUEN und teils bei einer Bundesstelle liegt. Soweit es sich zu großen Teilen um ein nicht öffentlich betretbares Waldgebiet handelt, ist dort der Einsatz von Videoüberwachung durch eine öffentliche Bundesstelle aus Sicht des TLfDI datenschutzrechtlich nicht problematisch. Wenn ein bestimmtes Gebiet für die Öffentlichkeit erkennbar gesperrt ist, muss dort im Regelfall nicht von einem überwiegenden schutzwürdigen Interesse des von der Videoüberwachung Betroffenen ausgegangen werden. Bei den öffentlich zugänglichen Waldgebieten kommt als Rechtsgrundlage für eine Videoüberwachung lediglich § 6b Abs. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke, nämlich der Berichtspflicht an die öffentlichen Stellen nachkommen zu können, in Betracht. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da die Beobachtung eines Wolfes im öffentlichen Interesse liegt, kann das schutzwürdige Interesse betroffener Spaziergänger, die durch Zufall eine Wildkamera auslösen, zurücktreten. Allerdings gilt die Rechtsgrundlage nur für nichtöffentliche Stellen, also für private Jagdpächter oder den Besitzer des Waldstückes.

Soll für Zwecke des Monitorings durch das Land als öffentliche Stelle eine Beobachtung zur Feststellung des Bewegungsradius' eines Wolfes stattfinden, kommt § 25a Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) als Rechtsgrundlage in Betracht. Danach ist die Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Be-

troffenen überwiegen. Ein Hausrecht des Landes in den Jagdgebieten, die im gemischten Eigentum stehen, besteht jedoch nicht. Da sich vorliegend die Videoüberwachung also nicht auf § 25a Abs. 1 ThürDSG stützen kann, wird die Videoüberwachung als wissenschaftliches Monitoring im Auftrag des Freistaats Thüringen auf der Grundlage von § 8 ThürDSG in Verbindung mit § 6 BNatSchG von nach § 7 BNatSchG streng geschützten Arten durchgeführt.
Aus Gründen der Transparenz für potentiell betroffene Waldspaziergänger muss auf die Videoüberwachung und die entsprechenden Rechtsgrundlagen sowie die verantwortliche Stelle deutlich sichtbar an den Zugängen zu dem betreffenden Waldstück hingewiesen werden. Das TMUEN hat nach Rücksprache mit dem TLfDI eine ausführliche Handlungsanleitung entworfen, die den o. g. Kamerabetreuern genaue Anweisungen gibt, wie mit den Aufnahmen der Kameras umzugehen ist. Insbesondere sind Aufnahmen von zufällig erfassten Spaziergängern ohne weitere Auswertung sofort zu löschen. Der vom TMUEN vorgeschlagene Inhalt des Hinweisschildes für die betroffenen Waldbesucher entsprach den Erfordernissen.

Der Einsatz von Videoüberwachung ist für öffentliche Stellen des Freistaats Thüringen ausschließlich zur Wahrnehmung des Hausrechts im eigenen Zuständigkeitsbereich zulässig. Ohne eine spezielle Rechtsvorschrift, die die Videoüberwachung zur Tierbeobachtung für naturschutzrechtliche Zwecke in öffentlich zugänglichen Bereichen ausdrücklich erlaubt, ist der Einsatz von Wildkameras nur ausnahmsweise und nur unter sehr engen Bedingungen zulässig. Auf der Grundlage von § 8 ThürDSG in Verbindung mit § 6 BNatSchG kann im Auftrag des Freistaats Thüringen die Videoüberwachung von nach § 7 BNatSchG streng geschützten Arten als wissenschaftliches Monitoring durchgeführt werden.

Globalization computer technology – © red150770 / Fotolia.com

13 Wirtschaft, Wissenschaft und digitale Gesellschaft

13.1 Auch Handwerkskammer unterliegt Auskunftsanspruch

Ein Handwerkskammermitglied wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass die für ihn zuständige Handwerkskammer (HWK) ihm trotz mehrerer Wochen Wartezeit keine Auskunft über die zu seiner Person gespeicherten Daten erteilte. Daraufhin schrieb der TLfDI die HWK an und forderte diese auf, dem Betroffenen gemäß § 13 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ohne unzumutbare Verzögerung Auskunft zu erteilen über die dort zu seiner Person verarbeiteten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind. Obwohl die HWK kurz darauf die Erledigung der Angelegenheit mitteilte, meldete sich der Betroffene erneut beim TLfDI, da er immer noch keine Auskunft über die zu seiner Person gespeicherten Daten erhalten habe. Wie sich bei der daraufhin vom TLfDI nochmals kontaktierten HWK herausstellte, hatte diese das Kammermitglied zwar über die entsprechenden Rechtsgrundlagen unterrichtet, die die Verarbeitung seiner personenbezogenen Daten erlaubten, die konkreten Daten wurden dabei

aber nicht aufgeführt. Der TLfDI forderte die HWK auf, dies unverzüglich beim Betroffenen nachzuholen, was bald darauf auch von der HWK bestätigt wurde.

Das Auskunfts- und Einsichtsrecht des Betroffenen gemäß § 13 ThürDSG ist als eine der datenschutzrechtlichen Kernforderungen anzusehen. Hierdurch kann sich der Betroffene Kenntnis von den ihn betreffenden Datenverarbeitungsvorgängen verschaffen. Die öffentlichen Stellen haben zu beachten, einem solchen Antrag auf Auskunft und Akteneinsicht zeitnah und umfassend nachzukommen.

13.2 Datenübermittlung einer Handwerkskammer ohne Einverständnis des Betroffenen

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Übermittlung seiner Mobilfunknummer seitens der Handwerkskammer an Dritte. Nach Schilderung des Betroffenen beantragte dieser daraufhin bei der Handwerkskammer Auskunft nach § 13 Thüringer Datenschutzgesetz (ThürDSG) über die zu seiner Person dort gespeicherten Daten, die er aber nicht erhielt. Der TLfDI schrieb daraufhin die Handwerkskammer an und bat um Auskunft zum Sachverhalt. In ihrer Stellungnahme führte die Handwerkskammer aus, dass die Mobilfunknummer an einen ehemaligen Dozenten des Beschwerdeführers herausgegeben wurde. Danach wollte sich dieser Dozent mit dem ehemaligen Lehrgangsteilnehmer über den Inhalt des Lehrgangs unterhalten. Die Handwerkskammer hatte es versäumt, vorab den Betroffenen um seine Einwilligung in die Datenübermittlung zu ersuchen. Die Kammer versicherte, dass es sich um einen bedauerlichen Einzelfall gehandelt habe. Dem TLfDI wurde Auskunft zu den Datenarten gegeben, die über den Beschwerdeführer bei der Handwerkskammer gespeichert waren. Der Grund der gespeicherten Daten ergab sich danach aus einer von dem Beschwerdeführer dort absolvierten Fortbildungsprüfung. Der TLfDI forderte die Kammer auf, den Vorfall zum Anlass zu nehmen und die Kammermitarbeiter nochmals darüber zu unterrichten, dass personenbezogene Daten nur zur Erfüllung der erforderlichen Zwecke genutzt werden und nicht ohne ausdrückliches Einverständnis des Betroffenen an Dritte übermittelt werden dürfen. Nach Angaben der Handwerkskammer wurde in einer Dienstberatung der Sachverhalt zum Anlass genommen, die

verantwortlichen Mitarbeiter über die Einhaltung der datenschutzrechtlichen Vorschriften zu belehren. Der TLfDI informierte den Beschwerdeführer abschließend über die Stellungnahme der Handwerkskammer und die zu seiner Person gespeicherten Datenarten. Ob die Handwerkskammer auch dem Betroffenen noch die erforderliche Auskunft nach § 13 ThürDSG erteilte, ist dem TLfDI nicht bekannt. Der TLfDI sah im Ergebnis von einer Beanstandung der Handwerkskammer ab, da diese den Fehler sofort eingeräumt hatte, alle Mitarbeiter nochmals über die Einhaltung datenschutzrechtlicher Vorschriften belehrt hatte und im Übrigen versicherte, dass es sich lediglich um einen Einzelfall gehandelt habe.

Eine Handwerkskammer darf ebenso wie jede andere öffentliche Stelle personenbezogenen Daten an Dritte nur dann übermitteln, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt. In allen anderen Fällen ist der Betroffene um seine Einwilligung in die Datenübermittlung zu ersuchen. Weiterhin hat die Daten verarbeitende Stelle dem Betroffenen nach § 13 ThürDSG auf Antrag ohne zumutbare Verzögerung Auskunft über die zu seiner Person verarbeiteten Daten sowie weitere dort genannte Sachverhalte zu erteilen.

13.3 Widersprechende Angaben zur Einhaltung des Datenschutzes bei der GFAW mbH Erfurt

Ein Unternehmensgründer beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den unzulässigen Umgang mit seinen personenbezogenen Daten seitens der Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW Thüringen). Nach Schilderung des Betroffenen habe er im Rahmen der Beantragung des vom Europäischen Sozialfonds für Deutschland (ESF) geförderten Existenzgründerpasses gemäß der damaligen GFAW-Richtlinie termingerecht seine Teilnahme an den zu absolvierenden Beratungen (z. B. von Steuerberatern, Rechtsanwälten, Marketingberatern usw.) mit Originalbelegen nachgewiesen. Ihm seien danach auch die Fördermittel ausgezahlt worden. Daraufhin habe die GFAW vom Betroffenen verlangt, geeignete Nachweise für die tatsächlichen Zahlungen in Form von Originalquittungen oder Originalkopien von Kontoauszügen vorzulegen. Die GFAW habe dem Unternehmensgründer

mitgeteilt, dass die vorgelegten, in einigen Teilen unkenntlich gemachten Kontoauszüge zur Prüfung nicht ausreichen würden und nur ungeschwärzte Kontoauszüge vorzulegen seien. Darüber hinaus beschwerte sich der Betroffene darüber, dass er ein Gespräch zur Klärung der genannten Angelegenheit neben dem Eingangsbereich der GFAW habe führen müssen, sodass alle ankommenden Besucher die Möglichkeit gehabt hätten, den vertraulichen Inhalt des Gespräches zu verfolgen. Der TLfDI wandte sich deshalb an die GFAW und bat um Stellungnahme zu dem vom Betroffenen vorgetragenen Sachverhalt. Im Antwortschreiben der GFAW bestritt diese, dass vom Betroffenen ungeschwärzte Kontoauszüge verlangt worden wären. Vielmehr habe der Zuwendungsempfänger im Rahmen der Abrechnung von Fördermitteln Kopien von Kontoauszügen eingereicht. Tatsächlich sei es nicht um die Unkenntlichmachung von Zahlungsvorgängen gegangen, die mit der Förderleistung in keinem Zusammenhang stehen, sondern um den Umstand, dass der GFAW anstelle der Originale nur Kopien vorgelegt worden sein sollen. Die GFAW habe dem Zuwendungsempfänger diesen Unterschied mehrfach erläutert und diesen auf die für die Förderung geltenden Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P), die Bestandteil der Verwaltungsvorschriften zu § 44 Thüringer Landeshaushaltsordnung sind, hingewiesen. Hiernach seien zum Nachweis der Verwendung die Originalbelege vorzulegen, wobei es den Zuwendungsempfängern dabei unbenommen bleibe, die Originale zu schwärzen oder abgedeckt vorzulegen. Dem Zuwendungsempfänger wurde daher auch mehrfach angeboten, anstelle der Übersendung der Originalkontoauszüge diese unter Abdeckung der für die Förderung nicht relevanten Vorgänge zur Einsichtnahme vorzulegen. Eine unzulässige Erhebung personenbezogener Daten liege deshalb nicht vor. Zum zweiten vom Betroffenen geäußerten Vorwurf der nicht gewährleisteten Vertraulichkeit von Gesprächen, verwies die GFAW zunächst darauf, dass persönlich abgegebene Unterlagen am Empfang von Mitarbeitern entgegengenommen würden. Der zuständige Mitarbeiter werde hierzu im Regelfall nicht hinzugezogen. Wenn bei einem Zuwendungsempfänger Beratungs- oder Klärungsbedarf bestehe, erfolge vorab eine Terminvereinbarung mit dem zuständigen Sachbearbeiter. Die Terminvereinbarung erfolge dann in Abhängigkeit von der Verfügbarkeit der Beratungsräume und finde zum Schutz von vertraulichen Daten nicht am Empfang statt. Vorliegend sei der Beschwerdeführer jedoch ohne vorherige

Terminvereinbarung in der GFAW erschienen, da er lediglich Unterlagen abgeben wollte. Jedoch bat der Betroffene die Mitarbeiter des Empfangsbereiches um die persönliche Abgabe der Unterlagen, weshalb umgehend die für den Fall zuständige Sachbearbeiterin am Empfang erschienen sein soll. Diese habe dem Betroffenen mitgeteilt, dass die Unterlagen als Kopie nicht anerkannt werden können und auf die Notwendigkeit von Originalbelegen hingewiesen. In solchen „Ad-hoc Fällen“ werde die Sitzgruppe im Servicebereich abseits des Empfangstresens genutzt. Diese besitzt einen Sichtschutz, damit Dritte keine Einsicht in die Unterlagen eines Zuwendungsempfängers erlangen. Ebenso stelle der Abstand zum Tresen des Empfangs sicher, dass Gespräche in normaler Zimmerlautstärke vom Empfangstresen aus nicht ohne Weiteres mitgehört werden können. Im Ergebnis waren sowohl die Schilderungen des Beschwerdeführers als auch die Stellungnahme der GFAW als plausibel anzusehen. Da die dem TLfDI zur Verfügung stehenden Aufklärungskompetenzen mithin erschöpft waren, war es nicht möglich, den Vorgang abschließend zu klären. Einen datenschutzrechtlicher Verstoß seitens der GFAW konnte der TLfDI nicht feststellen. Dem Beschwerdeführer wurde das für ihn sicherlich nicht zufriedenstellende Ergebnis mitgeteilt. Er hat sich daraufhin aber nicht mehr gemeldet.

Die Pflicht des Zuwendungsempfängers zur Vorlage von Originalbelegen bei der GFAW ergibt sich für zahlreiche Förderleistungen aus den Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P). Wenn bestimmte Vorfälle von einem Betroffenen einerseits und einer Daten verarbeitenden Stelle anderseits unterschiedlich dargestellt werden, die dem TLfDI beide plausibel erscheinen, so kann kein datenschutzrechtlicher Verstoß der Stelle festgestellt werden.

13.4 Gewerbedaten im Internet – nicht für unsichere Drittstaaten bestimmt!

In seinem zehnten Tätigkeitsbericht (hier unter Gliederungspunkt 5.30) hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ausgeführt, dass eine Übermittlung der Grunddaten Name/Firma, Tätigkeit und Anschrift gemäß § 14 Abs. 5 Satz 2 Gewerbeordnung (GewO) innerhalb eines Land-

ratsamtes vom Gewerbeamt an die Wirtschaftsförderung zulässig sei, nicht jedoch deren Veröffentlichung im Internet.
Zu dieser Rechtsauffassung des TLfDI äußerte sich im März 2015 das Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) dahin gehend, dass die Übermittlung der o. g. Grunddaten über das Internet nicht gegen das Thüringer Datenschutzgesetz verstoße.
Das TMWWDG begründete seine Auffassung, die in diesem Sinne auch vom Bund-Länder-Ausschuss „Gewerberecht“ vertreten werde, im Kern damit, das nach Art. 8 Abs. 2 Buchstabe e. der EU-Datenschutzrichtlinie 95/46/EG ein Schutz personenbezogener Daten dann nicht erforderlich sei, wenn der Betroffene sie selbst öffentlich bekannt mache. Um einen solchen Fall handele es sich nach Auffassung des TMWWDG auch bei den o. g. Grunddaten, da die Gewerbetriebe diese ohnehin im Rechtsverkehr für jedermann offenlegen würden. Zudem seien diese Daten auch im Handelsregister einsehbar.
Weiterhin wies das TMWWDG darauf hin, dass die Dienstleistungsrichtlinie 2006/123/EG in Art. 22 Abs. 1 die Mitgliedstaaten verpflichte, sicherzustellen, dass ein Dienstleistungserbringer Informationen über seinen Namen, seinen Rechtsstatus, seine Rechtsform, seine Anschrift und Informationen darüber, wie eine schnelle Kontaktaufnahme und direkte Kommunikation mit ihm zu ermöglichen sei, zur Verfügung stellen müsse.
Nach eingehender Prüfung der Angelegenheit teilte der TLfDI dem TMWWDG mit, dass er an seiner bisherigen Rechtsauffassung festhalte. Grund hierfür war, dass die Voraussetzungen für eine Datenübermittlung in unsichere Drittstaaten gemäß § 23 Abs. 1 Satz 2 oder Abs. 2 ThürDSG im konkreten Fall gerade nicht vorlagen. Auch vor dem Hintergrund des Safe-Harbor-Urteils des EuGHs vom 6. Oktober 2015 zeige sich die Wichtigkeit des Ausschlusses von Datenübermittlungen in datenschutzrechtlich unsichere Drittstaaten.

Der Grundsatz des Übermittlungsverbots von personenbezogenen Daten in unsichere Drittstaaten, wie er in § 23 ThürDSG zum Ausdruck kommt, kann nur durch normenklare spezialgesetzliche Ausnahmenregelungen durchbrochen werden. Solange diese nicht existieren, hält der TLfDI an seiner Auffassung fest, dass auch Gewerbegrunddaten nicht im Internet veröffentlicht werden dürfen. Die Safe-

Harbor-Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 bestätigt diese Auffassung.

13.5 Verarbeitung von Teilnehmerdaten bei EU-geförderten Projekten

Die EU fördert etliche Bildungsmaßnahmen. Allerdings muss geprüft werden, ob die zur Verfügung gestellten EU-Mittel auch zweckentsprechend eingesetzt wurden. Dazu müssen personenbezogene Daten von Teilnehmern erfasst und verarbeitet werden. Das ist altbekannt. Die technische Entwicklung macht aber auch vor der EU-Förderung nicht Halt. Die EU forderte daher eine Umstellung auf elektronische Verfahren. Diesem Anliegen nahm sich das Thüringer Ministerium für Wirtschaft und Arbeit und Technologie (TMWAT, heute TMWDDG) zuständigkeitshalber an. Es entwickelte das Projekt „Datenschutz und Fraud-Management im eCohesion-Projekt der Operationellen Programme EFRE/ESF“. Fraud-Management bezeichnet übersetzt Technologien zur Betrugserkennung, e-Cohesion bedeutet die weitgehende elektronische Umsetzung der Abwicklung der Strukturförderung. In diesem Verfahren sollen neue IT-gestützte Arbeitsabläufe entstehen, Betrugsfälle leichter aufgedeckt und eine Effektivitätskontrolle ermöglicht werden. Wird ein Projekt bzw. eine Maßnahme aus Mitteln des Europäischen Sozialfonds (ESF) mitfinanziert, bestehen für die im TMWWDG angesiedelte Verwaltungsbehörde Berichtspflichten gegenüber europäischen Institutionen. Hierfür werden personenbezogene Daten der Teilnehmer an den Maßnahmen benötigt.
Das damalige TMWAT beteiligte hierzu den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser stellte fest, dass Grundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verbindliche Rechtsvorschriften der Europäischen Union waren. Hier sind die Verordnungen VO (EU) Nr. 1303/2013 und VO (EU) Nr. 1304/2013, insbesondere der Anhang I, der die zu erfassenden Daten näher bestimmt, und das Operationelle Programm des Europäischen Sozialfonds für die Förderperiode 2014 bis 2020, in welchem festgelegt wurde, mit welchen Indikatoren die Ergebnisse der Förderung gemessen werden, maßgeblich. Da die Gewährung der finanziellen Mittel nach diesen Vorschriften von der vorgeschriebenen Berichterstattung abhängt, wird auch die Teilnahme an der Maßnahme von der voll-

ständigen Angabe der erforderlichen personenbezogenen Daten abhängig gemacht. Hierzu wurde vom zuständigen Ressort ein Erhebungsbogen erarbeitet. Bei Eintritt in das Projekt werden Angaben zur persönlichen und beruflichen Situation der Teilnehmer erhoben. Hierzu gehören auch Fragen zu Behinderungen oder zum Migrationshintergrund Die Beantwortung dieser beiden Fragen ist freiwillig, eine fehlende Angabe führt nicht zum Ausschluss von der Maßnahme. Wenn die Maßnahme beendet ist, werden auch noch Angaben zur veränderten beruflichen Situation und zum Bildungsabschluss erhoben. Sechs Monate nach Austritt des Teilnehmers aus dem Projekt wird dann stichprobenmäßig von der Verwaltungsbehörde (im Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie [TMASGFF]) bei den Teilnehmern eine weitere Befragung zur beruflichen Situation durchgeführt. Mit der Durchführung der Datenerhebung wird der jeweilige Träger des Projekts beauftragt, der die datenschutzrechtlichen Vorgaben einzuhalten hat. Er darf die Daten also nur zu dem vorgegebenen Zweck erheben und verarbeiten. Im Auftrag des nach dem Regierungswechsel zuständigen TMASGFF werden die Daten über das Portal der Gesellschaft für Arbeits- und Wirtschaftsförderung (GFAW) erfasst und bei der Thüringer Aufbaubank (TAB) in einer Datenbank gespeichert. Der Europäischen Kommission wird durch das TMASGFF in Erfüllung der Berichtspflichten eine Zusammenfassung ohne Namen und Adressen der Teilnehmer übermittelt. Der Personenbezug in der bei der TAB geführten Datenbank ist für eine Zuordnung zum Zweck der oben erwähnten späteren Befragung nach sechs Monaten erforderlich.

Der TLfDI hat den Fragebogen auf dem Teilnehmerportal aus dem datenschutzrechtlichen Blickwinkel überprüft. Wichtig war vor allem die Aufklärung der von der Datenerhebung Betroffenen (=Teilnehmer), um die doch schwierige und komplexe Angelegenheit transparent zu machen. Jeder muss erkennen können, zu welchem konkreten Zweck er welche konkreten Daten anzugeben hat und zu welchem Zweck sie durch wen weiter verarbeitet werden. Eindeutig muss auch erkennbar sein, welche Daten Pflichtangaben sind, welche Angaben freiwillig gemacht werden können und welche Rechtsfolgen eine fehlende Angabe hat.

Den Anregungen und Forderungen des TLfDI wurde in diesem Zusammenhang vollständig nachgekommen. Damit ist auch wichtige Vorarbeit geleistet, denn diese Art der Datenverarbeitung soll in

Zukunft auf weitere Anforderungen von Daten nach Europäischen Vorschriften ausgeweitet werden.

Besonders bei der Umstellung auf automatisierte Verfahren zur Datenerhebung und -verarbeitung kommt der Aufklärung der Betroffenen erhebliche Bedeutung zu. Jeder muss erkennen können, zu welchem konkreten Zweck er welche konkreten Daten anzugeben hat und zu welchem Zweck sie durch wen weiterverarbeitet werden. Eindeutig muss auch erkennbar sein, welche Daten Pflichtangaben sind, welche Angaben freiwillig gemacht werden können und welche Rechtsfolgen eine fehlende Angabe hat.

13.6 Feuer (daten-) frei – Datenerhebung beim Bezirksschornsteinfeger

Die Schornsteinfegerinnung Thüringen informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass eine Untere Immissionsschutzbehörde plane, bei den Bezirksschornsteinfegern in zahlreichen Fällen personenbezogene Daten von Eigentümern, die Feuerungsanlagen betreiben, zu erheben. Aus datenschutzrechtlicher Sicht ist ein solches Übermittlungsersuchen jedoch nach derzeitigem Kenntnisstand des TLfDI unzulässig und daher von den Bezirksschornsteinfegern abzulehnen. Eine Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 Thüringer Datenschutzgesetz (ThürDSG) – [Rechtsvorschrift, Einwilligung, im Interesse des Betroffenen liegend, allgemein zugängliche Quellen, Strafverfolgung usw.] zulassen würden. Nach Auffassung des TLfDI ist die Zulässigkeit bereits deshalb nicht gegeben, weil die Datenerhebung nicht zur Erfüllung der in der Zuständigkeit des Bezirksschornsteinfegers und der Unteren Immissionsschutzbehörde liegenden Aufgaben erforderlich ist. Es gibt weder eine Rechtsgrundlage für das personenbezogene Erheben der vom Bezirksschornsteinfeger festgestellten Messwerte der Feuerungsanlagen, noch ist die Überprüfung der rechtmäßigen Durchführung der dem Bezirksschornsteinfeger zugewiesenen Aufgaben zur Erfüllung der Aufgaben der Unteren Immissionsschutzbehörde erforderlich. Aus der Ersten Verordnung zur Durchführung des Bundesimmissi-

onsschutzgesetzes ergibt sich, dass der Bezirksschornsteinfeger die Feuerstättenschau für die Feuerungsanlagen vornimmt. Somit erfolgt die Überwachung grundsätzlich durch den Bezirksschornsteinfeger. Dieser hat dem Eigentümer einer Feuerstätte Mängel an kehr- und überprüfungspflichtigen Anlagen mitzuteilen und zur Behebung innerhalb von sechs Wochen aufzufordern. Erst wenn der Eigentümer einer Feuerungsanlage der Behebung des Mangels nicht nachkommt, hat der Bezirksschornsteinfeger den Mangel der zuständigen Behörde anzuzeigen (§ 5 Abs. 1 Schornsteinfeger-Handwerksgesetz). Zusammenfassend ist festzuhalten, dass die Untere Immissionsschutzbehörde nicht ohne begründete Anhaltspunkte den Bezirksschornsteinfeger auffordern darf, ihr personenbezogen alle Eigentümer einer Feuerungsanlage einschließlich der technischen Daten der Anlage sowie der dort gemessenen Werte vorzulegen. Dies stellt zum einen alle Feuerstättenbetreiber unter einen gewissen Generalverdacht, und zum anderen ist gegebenenfalls hier auch ein Misstrauen gegenüber den Bezirksschornsteinfegern dahingehend abzuleiten, ob diese ihrer Anzeigepflicht nachkommen. Gegen eine Übermittlung von statistischen Daten zu Feuerungsanlagen (Alter, Leistung, Immissionswerte usw.) bestehen aus datenschutzrechtlicher Sicht hingegen keine Bedenken. Eine endgültige Stellungnahme der betroffenen Unteren Immissionsschutzbehörde hinsichtlich des dort Veranlassten steht noch aus. Diese wurde vom TLfDI bereits mehrfach angemahnt und steht kurz vor der Beanstandung wegen mangelnder Unterstützung nach § 38 Abs. 1 Nr. 1 ThürDSG.

Die bevollmächtigten Bezirksschornsteinfeger führen als beliehene Unternehmer in den ihnen anvertrauten Kehrbezirken hoheitliche Tätigkeiten aus. Eine Übermittlung von personenbezogenen Daten der Feuerstättenbetreiber an die Untere Immissionsschutzbehörde, ohne dass eine Rechtsvorschrift dies eindeutig vorsieht, ist unzulässig. Nur wenn ein Bezirksschornsteinfeger einen Feuerstättenmangel dort anzeigt, dürfen die erforderlichen personenbezogenen Daten an die Untere Immissionsschutzbehörde übermittelt werden.

Dozent hilft Studierenden © Robert Kneschke / Fotolia.com

14 Bildung, Jugend, Sport

14.1 Arbeitskreis (AK) Datenschutz und Bildung

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) tagte der Arbeitskreis Datenschutz und Bildung im vorliegenden Berichtszeitraum dreimal in Erfurt. Um einige wichtige Punkte herauszugreifen, die in den Sitzungen behandelt wurden, soll zunächst auf Projekt „Young Data“ verwiesen werden (siehe dazu Nummer 14.16). Die anwesenden Arbeitskreismitglieder diskutierten darüber, auf welche Weise das Jugendportal in die Verantwortung der Datenschutzbeauftragten des Bundes und der Länder übergeben werden kann. Unter anderem wurde hierbei festgelegt, wie sich die finanzielle Unterstützung des Bundes und der Länder gestaltet. Darüber hinaus wurden an den Bund und die Länder Arbeitsaufgaben hinsichtlich der inhaltlichen Betreuung der Menüpunkte des Internetauftritts verteilt. Weitere Punkte waren die formale Gestaltung von bestimmten Menüpunkten und die Klärung der presserechtlichen Verantwortlichkeiten für den Inhalt von „Young Data“. Die Seite ging dann als gemeinsames Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes

und der Länder anlässlich des Safer Internet Day am 10. Februar 2015 recht erfolgreich an den Start. Der Arbeitskreis beschäftigte sich auch mit dem Thema „Medienkunde als Schulfach“ und hier schwerpunktmäßig mit der Umsetzung des im Beschluss der Kultusministerkonferenz (KMK) zur Medienbildung in der Schule vom 8. März 2012 geäußerten Willens, dass Medienbildung in Lehrplänen und in der Lehrerausbildung verbindlich festgeschrieben werden sollte. Es wurde aus dem Arbeitskreis vorgeschlagen, einen medienpolitischen Kongress zu dieser Problematik durchzuführen. Man einigte sich dann darauf, dass der TLfDI zum Safer Internet Day am 10. Februar 2015 eine derartige Veranstaltung durchführt. Der TLfDI organisierte daraufhin eine Fachtagung unter Beteiligung zahlreicher Experten auf dem Gebiet der Medienkompetenz und zahlreicher interessierter Zuschauer (siehe hierzu Anlage 48). Auf Einladung des TLfDI nahm auch der frühere Staatssekretär des ehemaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur Stellung zum Stand der Vermittlung von Medienkompetenz in den Thüringer Schulen und hob hierbei auch die Wichtigkeit der Berücksichtigung dieses Themas in der grundständigen Lehrerausbildung vor. Er verwies diesbezüglich auf den dabei geplanten Ausbau in Kooperation mit dem TLfDI. Der TLfDI erwähnte in diesem Zusammenhang, dass der Beschluss der KMK aus dem Jahr 2012 in den Ländern aus Sicht der Landesdatenschutzbeauftragten nicht hinreichend umgesetzt werde und eine Evaluierung der gegenwärtigen Standards bei der Umsetzung von Medienbildungskonzepten im Schulunterricht und in der Lehrerausbildung nicht stattfinde.

Weiterhin tauschten sich die Arbeitskreismitglieder darüber aus, wie das Thema Medienbewusstsein tatsächlich unter die Menschen gebracht werden könne. Die Landesdatenschutzbeauftragten berichteten hierzu über ihre Aktivitäten in Form von Veranstaltungen, Vorträgen, Aktionen, Kampagnen usw., um die Wichtigkeit des Anliegens herauszustellen. Der TLfDI berichtete von seiner Idee, die Abgeordneten für die Sache zu interessieren und z. B. einen runden Tisch zusammen mit Informatikern, Datenschützern und auch Lehrern zu installieren.

Zur Arbeitskreissitzung am 1. Dezember 2015 hatte der TLfDI zum Thema „Medienbildung in der Schule“ unter Berücksichtigung des Beschlusses der Kultusministerkonferenz mehrere Fachleute eingeladen, die zu dem Thema sachkundig Stellung nehmen konnten. Die

Staatssekretärin des Thüringer Ministeriums für Bildung, Jugend und Kultur berichtete, dass im Zusammenhang mit dem Beschluss der Kultusministerkonferenz vom 8. März 2012 eine Arbeitsgruppe auf Staatssekretärsebene eingerichtet wurde, die bereits erste Vorschläge zur Umsetzung der Forderungen des Beschlusses entwickelt habe. Es sei geplant, bis Ende des Jahres 2016 ein Ergebnis vorzulegen. Zur Situation in Thüringen verwies die Staatssekretärin auf die externe Evaluation des Kurses Medienkunde, die vom TLfDI unterstützt werde. Es gebe auch einen „Runden Tisch Medienkompetenz“ als interministerielle Arbeitsgruppe, die für eine bessere Vernetzung sorgen solle. Ein Ergebnisbericht an den Thüringer Landtag sei für das Jahr 2017 geplant.

In einem weiteren Gastvortrag wurde die derzeitige Erarbeitung einer Strategie der Kultusministerkonferenz zur „Bildung in einer digitalen Welt“ bis Ende 2016 unter Einbeziehung der verschiedenen Kultusministerkonferenz-Ausschüsse vorgestellt. Danach werden dort Vorschläge erarbeitet, auf welche Weise die Lehrpläne der Schulen ergänzt werden müssen, um mehr Medienkompetenz zu schaffen. Es soll eine bundesweite Verständigung über gültige verbindliche Anforderungen in den Bereichen der Qualifizierung von Erziehenden und Lehrenden geben. Die Arbeitskreismitglieder signalisierten die Bereitschaft zum Dialog mit der Kultusministerkonferenz und begrüßten die künftige intensive Kooperation ausdrücklich. Der TLfDI als Vorsitzender des AK Datenschutz und Bildung wird nach Abschluss des Koordinierungsprozesses innerhalb des Generalsekretariats der Kultusministerkonferenz in die weitere Planung einbezogen werden. Die unmittelbare Zusammenarbeit der Kultusministerkonferenz mit dem Arbeitskreis Datenschutz und Bildung zum Thema „Medienbildung in der Schule“ stellt dabei ein Novum dar, von dem sich der TLfDI eine stärkere Einflussnahme des Datenschutzes auf die zukünftige Medienbildung in den Schulen verspricht.

In einem wissenschaftlichen Vortrag wurde der Einsatz von digitalen Medien in der Bildung beleuchtet. Die Vortragende plädierte dafür, dass digitale Medien und die pädagogische Arbeit besser verbunden werden und ein Lernen und Lehren mit digitalen Medien nicht reicht. Nur die Hälfte der Lehrenden schätze die Potentiale digitaler Medien. In Deutschland gebe es einen negativen Zusammenhang zwischen der Häufigkeit der Computernutzung in der Schule und digitalen Kompetenzen der Schüler. Nach einer Studie habe das Lernen

mit digitalen Medien im Schnitt einen relativ geringen nachweisbaren Effekt auf den Lernerfolg. Der Lernerfolg hänge danach eher von Faktoren wie Weiterbildung der Lehrkräfte, der Einbindung in Unterrichtskonzepte und der Art der eingesetzten Software ab. Schließlich verwies die Wissenschaftlerin auf die Notwendigkeit des Einsatzes von digitalen Medien als Bildungsmedien und stellte die Chancen dar, die der richtige Einsatz von digitalen Medien für Lernprozesse biete. Hierzu gehöre nicht nur das Lernen über die richtige Benutzung von digitalen Medien, sondern vielmehr das Verständnis und die Auseinandersetzung darüber, wie digitale Medien funktionieren. Lehrende sollen ein digitales Medium nicht nur von seiner Oberfläche und Funktion kennen, sondern auch die dahinter stehenden Prozesse wie Algorithmen berücksichtigen und dieses an die Schüler weitergeben. Es besteht die Forderung nach einer verpflichtenden Medienbildung für pädagogische Fachkräfte in der Jugend- und der Lehrerbildung sowie der entsprechenden Verankerung in den Schullehrplänen und in der beruflichen Bildung.
Insgesamt sieht der TLfDI den Arbeitskreis Datenschutz und Bildung weiterhin auf einem guten Weg. Die Vermittlung von Medienkompetenz durch Medienbildung bei Lehrern und Schülern, aber auch in der Bevölkerung insgesamt und die Stärkung des datenschutzrechtlichen Bewusstseins werden dem Arbeitskreis Datenschutz und Bildung als Schwerpunkthemen erhalten bleiben.

Der Arbeitskreis Datenschutz und Bildung hat weiterhin das Thema Datenschutz als Bildungsaufgabe als Schwerpunkt seiner Arbeit. Dabei stehen der Austausch der Arbeitskreismitglieder über Aktivitäten zur Förderung der Medienkompetenz und auch die aktive Beteiligung am fachlichen und politischen Prozess der Umsetzung dieses Ziels in den Ländern im Vordergrund. Die Kooperation des Arbeitskreises mit der Kultusministerkonferenz zu Fragen der Umsetzung von Medienbildung in Schule, Lehrerausbildung und Lehrerweiterbildung wird zukünftig erstmals die Möglichkeit bieten, den datenschutzrechtlichen Aspekt verstärkt einzubringen.

14.2 Unterarbeitskreis Datenschutz und Schule

Im vergangenen Berichtszeitraum fanden unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zwei weitere Sitzungen der Arbeitsgruppe

Datenschutz und Schule der Konferenz der Datenschutzbeauftragten des Bundes und der Schule, die nunmehr Unterarbeitskreis (UAK) Datenschutz und Schule des Arbeitskreises Datenschutz und Bildung heißt, statt. Nach wie vor herrscht in den Bundesländern an datenschutzrechtlichen Themen im Schulbereich kein Mangel. Dementsprechend wurden auf den Sitzungen zahlreiche Tagesordnungspunkte besprochen. Ein Schwerpunkt war die Einführung von Online-Lernplattformen an Schulen. Hierbei stellen die Schulen eine Software zur Verfügung, die für Unterrichtszwecke eingesetzt wird. Hierauf werden Lernmaterialien für den Zugriff abgelegt, Lernvorgänge organisiert und die Kommunikation zwischen den Lehrerinnen/Lehrern und den Schülerinnen/Schülern über das Internet ermöglicht. Inzwischen gibt es zahlreiche Anbieter von Online-Lernplattformen, die ihre Software den Schulen zur Nutzung anbieten. Die Landesdatenschutzbeauftragten berichteten dabei im Kollegenkreis über die Ergebnisse ihrer datenschutzrechtlichen Prüfung von bestimmten Online-Lernplattformen. Ebenfalls wurden jeweils die Rechtsgrundlagen vorgestellt, die das Betreiben von Online-Lernplattformen im eigenen Bundesland erlauben und entweder die Teilnahme hieran nur auf freiwilliger Basis gestatten oder aber die Nutzung des Systems als verpflichtend vorschreiben. Der UAK war sich einig darüber, dass ein solches System nur eingeführt werden darf, wenn die faktische Teilnahme der Lernenden hieran durch die Schule gewährleistet werden kann. Aufgrund der datenschutzrechtlichen Komplexität der Nutzung von Online-Lernplattformen erarbeitet der Arbeitskreis Datenschutz und Bildung zurzeit eine entsprechende Orientierungshilfe (siehe dazu Nr. 14.33.), die noch in diesem Jahr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgelegt werden wird und den Schulen dann zur Verfügung gestellt werden soll. Diese können sich anhand der Orientierungshilfe einen Überblick darüber verschaffen, welche datenschutzrechtliche Mindestkriterien sie in Online-Lernplattformen erfüllen müssen. Als weiteres großes Thema wird darüber diskutiert, dass Lehrer in zunehmendem Maße private Datenverarbeitungsgeräte für den Einsatz von schulischen Anwendungen nutzen. Gemeint sind hier die zahlreich angebotenen Apps, die es den Lehrkräften ermöglichen, ihre privaten mobilen Datenverarbeitungsgeräte für dienstliche Zwecke einzusetzen und hiermit personenbezogene Schüler-, Eltern- und Lehrerdaten zu verarbeiten. Im Ergebnis stellte der UAK fest, dass in den meisten Bundesländern, so auch in Thüringen,

noch keine Vorschriften bestehen, die speziell die dienstliche Nutzung von privaten mobilen Endgeräten regeln. Aus dem UAK hat sich eine Ad-Hoc-Arbeitsgruppe gebildet, die eine Handreichung „Einsatz von schulischen Anwendungen auf privaten Datenverarbeitungsgeräten bei Lehrkräften“ für Schulleiter und Lehrer erarbeitet hat (siehe dazu Nr. 14.40.) und diese ebenfalls noch in diesem Jahr den Schulen zur Verfügung stellen wird. Weiteres Thema des UAK war der Umgang mit Schülerdaten bei Kindern von beruflich Reisenden. Bedingt durch den ständigen Schulwechsel müssen unterschiedliche Schulen, die die Kinder jedes Jahr besuchen, auf die betroffenen Schülerdaten zugreifen. Die erforderlichen Datenflüsse zwischen der jeweiligen Stammschule dieser Schüler und den übrigen besuchten Schulen sowie die hierzu verwendete Software müssen datenschutzrechtlich begleitet werden. Im Zusammenhang mit den zahlreichen bundeslandübergreifenden Schul- und Bildungsuntersuchungen, zu denen in den meisten Bundesländern die Landesdatenschutzbeauftragten um eine datenschutzrechtliche Stellungnahme der jeweiligen Untersuchung gebeten werden, wurde aus Kreisen der Bildungsforscher der Vorschlag unterbreitet, das datenschutzrechtliche Prüfverfahren zu vereinfachen. In diesem Zusammenhang gab es auch einen Austausch über die gesetzlichen Bestimmungen in den einzelnen Ländern, wenn in wissenschaftlichen Schülerbefragungen auch Fragen enthalten sind, die den Kernbereich privater Lebensgestaltung betreffen. In manchen Bundesländern besteht die gesetzliche Regelung, dass die Beantwortung solcher Fragen nur mit Einwilligung der Betroffenen erfolgen darf. Einige Landesdatenschutzbeauftragte sind der Auffassung, dass auch mit ausdrücklicher Regelung eine Einwilligung zur Beantwortung der Fragen erforderlich ist, da hier die schutzwürdigen Belange des Betroffenen immer überwögen. In anderen Bundesländern existieren Verordnungen, die einen Datenkatalog enthalten, in dem geregelt ist, welche Daten erhoben werden dürfen. Besprochen wurden auch die neuen Entwicklungen im Schuldatenschutzrecht in den Ländern. Hier bauen einige Länder die dort bestehenden speziellen Schuldatenschutzverordnungen weiter aus und passen diese an die gegebenen technischen Entwicklungen an. Hinsichtlich einer Nutzung von sozialen Netzwerken für den Unterricht ergibt sich in den Ländern ebenfalls ein uneinheitliches Bild. Teilweise besteht von Kultusseite ein Verbot für schulische Kontakte über soziale Netzwerke zwischen den Lehrkräften und den Schülern, in anderen Fällen warnen Landesdatenschutzbeauftragte

generell vor einer Nutzung sozialer Netzwerke zu schulischen Zwecken und beraten hierzu die Schulen oder geben selbst erstellte Handreichungen heraus. Weitere Themen waren z. B. die Videoüberwachung an Schulen, das Erstellen von Videoaufnahmen im Unterricht, die Sozialarbeit an den Schulen, die schulische Nutzung von Cloud-Diensten, Datenübermittlung von den Schulen an die Jugendberufsagenturen, das Blockieren oder Orten von Mobilfunk durch Schulen bei Prüfungen usw. Es ist abzusehen, dass dem UAK Datenschutz und Schule die Arbeit nicht ausgehen wird.

Der UAK Datenschutz und Schule hat sich auch in den letzten zwei Jahren mit zahlreichen Datenschutzthemen auseinandergesetzt, die bei der Verarbeitung von Schüler-, Eltern- und Lehrerdaten durch die Schule entstehen. Durch den Austausch mit den Kollegen aus den anderen Bundesländern gewinnt der TLfDI wertvolle Hinweise für die eigene Arbeit im Schulbereich.

14.3 Medienbildung tut not – TLfDI sorgt für Futter!

„Wir haben nichts!“ – So schallte es dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bei seinen Besuchen in Thüringer Schulen entgegen. Der Hilfeschrei kam von Lehrern und bezog sich auf geeignete Unterrichtsmaterialien zu den Themen Datenschutz und Datensicherheit. Vor allem jene Lehrerinnen und Lehrer, die an der Umsetzung des Kurses Medienkunde beteiligt sind, fühlten sich alleingelassen. Dem TLfDI war natürlich klar, dass sich hier etwas tun muss und handelte, unter anderem, indem er einen Lehrer an seine Behörde holte, der sich darum kümmert. Seitdem ist einiges geschehen. Nach intensiver Internetrecherche waren schnell geeignete Videos, Broschüren usw. gefunden. Bei besonders geeigneten Materialien sorgte der TLfDI für die Nutzungsrechte für Thüringer Schulen. Die Angebote landeten dann umgehend in der Mediothek des Thüringer Schulportals zum kostenfreien Download. Links zu anderen Quellen im Netz füllen eine eigens beim TLfDI entwickelte Mediendatenbank. Sie erlaubt dem Lehrer, alters- und schlagwortspezifisch nach „Futter“ für seine Schüler zu suchen. Die Datenbank ist auf der Internetseite des TLfDI online. Dort ist auch schon ein Video abrufbar, das Teil eines komplexen Unterrichtsprojektes ist, das beim TLfDI selbst entwickelt wurde. In sechs Unterrichtsstunden können und sollen

sich Schüler im Rahmen des Sozialkundeunterrichts mit der Frage „Videoüberwachung – In Ordnung oder nicht?“ auseinandersetzen. Das umfangreiche Material ist so ausgearbeitet, dass ein Lehrer den Unterricht für seine Schüler auch dann erfolgreich gestalten kann, wenn er sich zuvor noch nicht mit diesem Thema beschäftigt hat. Erfolgreich sein heißt hier, dass die Jugendlichen ihre Sensibilität für den Wert des Grundrechts auf informationelle Selbstbestimmung und ihre Bürgerrechte entwickeln und „nebenbei“ auch ihre Medienkompetenz. Beide Aspekte sind dem TLfDI Grundanliegen, die er mit Nachdruck gegenüber den politisch Verantwortlichen in Thüringen und der Kultusministerkonferenz (KMK) vertritt. Denn hier besteht Handlungsbedarf in unserer digitalisierten Welt, insbesondere was die Befähigung der jungen Generation zur reflektierten(!) Interaktion mit Medien betrifft. Der Schutz von und der sensible Umgang mit personenbezogenen Daten sind hier zentrale Herausforderungen.

Der TLfDI setzt sich offensiv für Veränderungen in den Schulen ein. Unabdingbar ist auch, dass eine solide Medienbildung endlich in den Lehramtsstudiengängen der Hochschulen Eingang findet und zwar für alle Schulfächer aller Bildungsgänge. Der TLfDI fordert nicht nur, sondern hat dem Bildungsministerium konkrete Unterstützungsangebote unterbreitet, beispielsweise für die Einbindung von Datenschutz- und Datensicherheitsinhalten in die Lehrerausbildung an den Thüringer Studienseminaren. Darüber hinaus hat er seine Bereitschaft zur Mitwirkung bei der Evaluation des Kurses Medienkunde erklärt, die vom Bildungsministerium auch angenommen wurde.

Auch landesübergreifend engagiert sich der TLfDI für eine zeitgemäße Medienbildung. Auf einer KMK-Fachkonferenz im September 2015 stieß der TLfDI mit seinem Beitrag über den Datenschutz als Zukunftskompetenz im digitalen Zeitalter auf große Resonanz. In der Folge entwickelte sich eine Zusammenarbeit zwischen dem Arbeitskreis Datenschutz und Bildung der Datenschutzbeauftragten des Bundes und der Länder – dessen Vorsitzender der TLfDI ist – und Vertretern der KMK (siehe dazu Nr. 14.1).

Handeln ist angesagt! Strategiepapiere, an deren Umsetzung es häufig mangelt, gibt es bereits genug.

Datenschutzaspekte sind wesentlicher Bestandteil von Medienkompetenz. Der TLfDI sieht hier Handlungsbedarf und sorgt auf verschiedenen Ebenen dafür, dass sich etwas bewegt.

14.4 Medienschulen in Thüringen – kein Auslaufmodell!

„Thüringer Medienschule“ – mit Stolz brachten etliche Thüringer Schulen in den 2000er-Jahren ein solches Schild an’s Schulhaus an. Allen „draußen“ sollte es klar machen: Hier zieht das Informationszeitalter nicht an der Schultür vorbei, sondern hält Einzug in die Klassenräume und vor allem in die Köpfe von Lehrern und Schülern. 47 Schulen machten sich damals von 2000 bis 2006 auf den Weg und bildeten ein thüringenweites Netzwerk. Dabei waren Schulen aller allgemeinbildenden Schularten, angefangen von Grundschulen über Regelschulen, Gesamtschulen bis hin zu Gymnasien. Auch Förderschulen reihten sich ein, weil sie erkannten, dass eine möglichst solide Medienkompetenz für Beruf und gesellschaftliche Teilhabe unverzichtbar ist. Die beteiligten Schulen waren nicht allein. Sie erhielten Ausstattungsunterstützung. Zudem konnten sich die Lehrkräfte in zahlreichen zentralen Fortbildungen des Thüringer Instituts für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) und regional in den Schulamtsbereichen fortbilden. Die Medienschulen selbst strahlten mit ihren Erfahrungen in ihr regionales Umfeld aus. Alles in allem ein guter Anfang.

Was ist draus geworden? Sind inzwischen weitere Medienschulen hinzugekommen? – Diese Fragen standen 2015 auch auf der Agenda des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Bekanntermaßen steht dort die Medienkompetenzentwicklung der Thüringer Schülerinnen und Schüler ganz oben auf der Liste, denn Datenschutz und Datensicherheit sind heute ein untrennbarer Aspekt dieser Schlüsselqualifikation.

Anfragen beim Thüringer Ministerium für Bildung, Wissenschaft und Sport zeigten, dass der Schwung nachgelassen hat. Seit 2010 gibt es noch sieben offiziell geführte Medienschulen in ganz Thüringen. Man muss fragen, ob Initiativreichtum und Kraft dieser sieben besonders engagierten Schulen ausreichen können, um auf die anderen 811 allgemeinbildenden Schulen Thüringens (ohne Schulen in freier Trägerschaft) wirkungsvoll auszustrahlen. Das Ministerium teilte auf Anfrage des TLfDI mit, dass die Schulleiter eine stärkere Vernetzung wünschten und dass beim nächsten Thüringer Schulmedientag angesprochen werden soll, wie „im Rahmen unserer Möglichkeiten gezielter Unterstützung“ geleistet werden kann. Der TLfDI wird diesen Prozess nach Kräften unterstützen, auch im Rahmen

des im Oktober 2015 konstituierten „Runden Tisches Medienkompetenz“.

Der TLfDI stellt insgesamt fest, dass in puncto Medienkompetenz in Thüringen Aufbruchstimmung herrscht. Konzertiertes Vorgehen wird Thüringen auch hier wieder einen Spitzenplatz verschaffen. Medienschulen zeichnen sich durch besonderes Engagement für die Medienkompetenzentwicklung ihrer Schüler aus. Sie sind Impulsquelle für andere Schulen der Region.

14.5 Lernmanagementsystem neu denken!

Aufgrund des großen Engagements des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu dem Thema Medienkunde wurden im Berichtszeitraum zahlreiche allgemeine Anfragen aus dem Schulbereich an den TLfDI herangetragen. Die Schulen möchten einerseits auf Augenhöhe mit den Schülern kommunizieren und dafür die modernen Medien nutzen. Die gängigen sozialen Netzwerke bieten aber andererseits für den Schulbereich keine datenschutzgerechten Lösungen an. Daher versuchen etliche Schulen, eigene Lösungen zu finden. Im Zuge eines derartigen Projektes trat ein Lehrer an den TLfDI heran und bat um fachliche Begleitung. Im Gespräch stellte sich heraus, dass die Schule ein Open-Source-Lernmanagementsystem ins Auge gefasst hatte, das die Funktion sozialer Netzwerke abbilden und diese datenschutzkonform umsetzen sollte. Das System sei bereits von einem Landesbeauftragten für den Datenschutz begutachtet und für gut befunden worden. Diese Angaben konnten bei konkreter Nachfrage bei diesem Landesbeauftragten für den Datenschutz leider nicht bestätigt werden. Es stellte sich heraus, dass vermutlich der Datenschutzbeauftragte der Stelle, die das Lernmanagementtool entwickelt hatte, diese Prüfung vorgenommen hatte. Dem Lehrer wurde erklärt, dass der TLfDI gerne bereit ist, das Lernmanagementsystem zu prüfen, sofern die Schule sich für einen Einsatz entscheidet und den TLfDI um eine Prüfung bittet. Hierzu ist es im Verlauf des weiteren Verfahrens noch nicht gekommen.

Nach Auffassung des TLfDI besteht im Bereich der Lernmanagementsysteme Handlungsbedarf. Da bei der Kommunikation zwischen Schule und Schülern mit diesen Mitteln zahlreiche daten-

schutzrechtliche Probleme geklärt werden müssen, wird es künftig vermehrt Aufgabe des TLfDI sein, derartige Systeme auf die Vereinbarung mit den geltenden Datenschutzregeln zu prüfen.

14.6 Datenschutz im Hort

Die Mutter eines Schulkindes beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den in einer Stadtverwaltung herausgegebenen Erhebungsbogen zur Anmeldung eines Kindes im Schulhort. Insbesondere hielt die Beschwerdeführerin die Frage zur Angabe der genauen Hortbetreuungszeit und die Abfrage des Ermäßigungstatbestands, auch wenn dieser gar nicht genutzt werden sollte, für unzulässig. Bei der Berechnung der Hortgebühr wird das Einkommen der Eltern sowie die Zahl der kindergeldberechtigten Kinder in einer Familie berücksichtigt. Wer weiß, dass der Ermäßigungstatbestand nicht erfüllt wird und ohnehin die Höchstgebühr zu entrichten hat oder dies freiwillig tut, muss diesen Teil des Erhebungsbogens wegen mangelnder Erforderlichkeit nicht ausfüllen. Der TLfDI konfrontierte die verantwortliche Stadtverwaltung mit den von der Beschwerdeführerin angeführten Kritikpunkten und wies gleichzeitig auf § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) hin, wonach die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Nach § 4 der Thüringer Hortkostenbeteiligungsverordnung wird lediglich danach unterschieden, ob eine Betreuung von mehr oder weniger als 10 Stunden in der Woche erfolgen soll. Sofern ein Elternteil sein Kind für mehr als 10 Stunden in der Woche anmeldet, hat es Anspruch auf Betreuung während der gesamten Öffnungszeit des Hortes. Auf Grundlage dieser Vorschrift war es nicht zulässig, bei den Erziehungsberechtigten verpflichtend die genaue Zeit zu erheben, in der das Schulkind den Hort besucht.
Der TLfDI forderte die Stadtverwaltung deshalb zunächst auf, diese Angaben lediglich auf freiwilliger Basis zu erheben und dies im Erhebungsbogen deutlich zu kennzeichnen oder aber die Frage aus dem Formular herauszunehmen. Die Stadtverwaltung wies in ihrer Stellungnahme dann darauf hin, dass die erhobenen Daten alle zwei Jahre an das zu diesem Zeitpunkt zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) übermittelt werden mussten und insofern die Verantwortlichkeit für die Zulässigkeit

dieser Datenerhebung dort lag. Tatsächlich bat das TMBWK einige Zeit später den TLfDI und die Stadtverwaltung für die Klärung des Sachverhalts zu einem Gespräch. Aus diesem Gespräch ergab sich, dass die Stadtverwaltung als Schulträger im vorliegenden Fall nicht nach dem Thüringer Schulgesetz, sondern als Träger des Schulhortes handelte. Damit richtete sich die Zulässigkeit der Datenerhebung nach dem ThürDSG. Gemäß § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Zusätzlich wurden nach Nr. 4.2.2 der zu diesem Zeitpunkt gültigen Verwaltungsvorschrift des TMBWK vom 12. Dezember 2013 (Gz: 1B 4/4025) den Grund- und Gemeinschaftsschulen im Rahmen der dem Schulamt zur Verfügung gestellten Stellen die Erzieherwochenstunden für die Hortarbeit von den Schulämtern zugewiesen. In einer Planungsphase wurde zunächst ein durchschnittlicher Wert für die Berechnung des Erzieherbedarfs ermittelt, der dann zum Schuljahresbeginn endgültig abgeglichen wurde. Um die Zahl der benötigten Erzieher und die anfallende Betreuungszeit möglichst sachgerecht ermitteln zu können, war es für den Schulträger hilfreich zu wissen, zu welchen Zeiten ein Kind regelmäßig den Hort aufsucht. Hintergrund hierfür war die Teilnahme der Stadtverwaltung an einem Erprobungsmodell des Landes, welches seit mehreren Jahren durchgeführt wurde. Hier erstattete das Land den Trägern die Differenz, die zwischen dem für das Hortpersonal bereitgestellten Geld und dem tatsächlichen Bedarf bestand. Um den Differenzbetrag festzustellen, war es notwendig, dass der Schulträger Daten erhebt. Auch unter Berücksichtigung der vom TMBWK erlassenen, oben genannten Verwaltungsvorschrift, die sich an die Schulverwaltungsämter, nicht aber an die Bürger richtete, kam der TLfDI erneut zur Auffassung, dass die Antragsteller auf einen Schulhortplatz gesetzlich nicht verpflichtet waren, hierzu verbindliche Angaben zu machen. Gleichwohl hat der TLfDI auf eine Kennzeichnung dieser Frage als freiwillig verzichtet, da der Träger des Schulhortes zur Übermittlung der Summe der konkreten Stundenzahl einer Hortnutzung an das TMBWK verpflichtet war. Lediglich die nach der Thüringer Hortkostenbeteiligungsverordnung erforderliche Angabe, ob eine Betreuung von mehr oder weniger als 10 Stunden wöchentlich erfolgte, war durch die Eltern zu machen. Der Beschwerdeführerin wurden deshalb die Möglichkeiten aufgezeigt, der Stadtverwaltung entweder mittzuteilen, dass sie keine Angaben machen kann oder aufgrund der

Tatsache, dass ihr genaue Angaben nicht möglich sind, den Höchstbetreuungszeitraum anzugeben. Der TLfDI wies die Beschwerdeführerin darauf hin, dass die gemachten Angaben in keinem Fall Auswirkungen auf ihren Anspruch auf Betreuung des Kindes im Hort haben. Selbstverständlich bestand auch keine Verpflichtung, Angaben zur Ermäßigung der Hortgebühren zu machen, wenn eine Ermäßigung, aus welchen Gründen auch immer, nicht beantragt wird. Auf eine aktuelle Anfrage des TLfDI bei der Stadtverwaltung teilte diese mit, dass nach wie vor das nunmehr zuständige Thüringer Ministerium für Bildung, Jugend und Sport die benötigten Hortzeiten stundengenau im Rahmen des Erprobungsmodells erfragt. Der TLfDI hat die Stadtverwaltung aufgefordert, auf dem Erhebungsbogen die Frage nach der konkreten zeitlichen Inanspruchnahme des Hortes als freiwillig zu kennzeichnen.

In einem Erhebungsbogen zur Anmeldung für einen Betreuungsplatz im Schulhort dürfen nur diejenigen Daten erhoben werden, die für die Aufgabenerledigung des Aufgabenträgers unbedingt erforderlich sind. Sind bestimmte Daten der Antragsteller für den Träger oder wie im beschriebenen Fall für die Durchführung eines Erprobungsmodells erforderlich, ohne dass eine Rechtsgrundlage die Antragsteller hierzu verpflichtet, so müssen die Angaben nicht gemacht werden. Ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, ist der Betroffene hierauf hinzuweisen, wobei aber auch hier keine Auskunftspflicht besteht.

14.7 Schüler unter Beobachtung? – Videogaga 7

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über eine Berufsschule. Die Schule würde die Eingangsbereiche zu ihrem Grundstück und zum Gebäude videoüberwachen. Besonders störte den Beschwerdeführer, dass sich die Zugangsrampe, über die man statt der Treppe das Gebäude erreichen kann, im Aufnahmebereich der Kamera befand. Der TLfDI wandte sich an die Berufsschule und stellte die Fragen, deren Beantwortung zur datenschutzrechtlichen Prüfung der Videoüberwachung notwendig ist. Als die Antwort der verantwortlichen Stelle einging, ergab sich ein weiteres Problem: Der von der Schule verwendete Kopfbogen des Antwortschreibens legte nahe, dass es sich bei der Schule um ein Unternehmen handel-

te, an dem eine Stadt zumindest teilweise beteiligt war. Für das Tätigwerden des TLfDI ist wegen der anzuwendenden Rechtsgrundlagen entscheidend, ob es sich bei der verantwortlichen Stelle um eine öffentliche oder eine nicht-öffentliche Stelle handelt. Nach § 2 Abs. 2 des Thüringer Datenschutzgesetzes (ThürDSG) gelten als öffentliche Stellen auch juristische Personen oder sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine Gemeinde beteiligt ist. Nach § 26 ThürDSG gilt allerdings, dass für den Fall, dass öffentliche Stellen am Wettbewerb teilnehmen, grundsätzlich die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) anzuwenden sind. Der TLfDI ging zunächst davon aus, dass die Schule als Unternehmen zwar Aufgaben der öffentlichen Verwaltung wahrnahm, hierbei aber im Wettbewerb zu anderen Unternehmen stand und auf sie daher die Bestimmungen des BDSG mit Ausnahme des zweiten Abschnitts und des § 38 anzuwenden waren, § 26 ThürDSG. Mit der Einordnung als öffentliche Stelle hat der TLfDI nicht mehr die Handlungsmöglichkeiten des § 38 BDSG, nach dem er Anordnungen treffen und mittels Verwaltungszwang durchsetzen kann. Bei öffentlichen Stellen kann er festgestellte Verstöße gegen das Datenschutzrecht lediglich beanstanden und die zuständige Aufsichtsbehörde informieren. Die Schule äußerte sich bislang nicht zur möglichen Beteiligung der Stadt und wurde nochmals zur Äußerung aufgefordert, da sie trotz Erinnerung nicht reagierte. Der TLfDI wird an die Stadt herantreten, falls die Schule die gestellten Fragen nicht innerhalb der neu gesetzten Frist beantwortet.

Zur Zulässigkeit der Videoüberwachung ist Folgendes festzustellen: Auf dem Gelände der Schule befanden sich drei Kameras. Eine Aufzeichnung fand nur in der Zeit von 16:00 bis 06:30 Uhr und am Wochenende 24-stündig, also außerhalb der Öffnungszeiten, statt. Gegen den Aufnahmebereich einer Kamera bestanden keine datenschutzrechtlichen Bedenken, weil sie lediglich auf den Innenhof der Schule gerichtet war. Bei den anderen beiden Kameras waren aber jeweils Teile der öffentlichen Straße bzw. des Bürgersteigs auf den Aufnahmen zu erkennen. Die Aufzeichnungen hatten einen sehr geringen Auflösungsgrad, weswegen Personen nicht ohne Weiteres eindeutig zu erkennen waren. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Entscheidend ist daher, ob Personen, die sich im Aufnahmebe-

reich der Kamera befinden, zumindest bestimmbar sind. Dies hielt der TLfDI auch bei der geringen Auflösung nicht für grundsätzlich ausgeschlossen. Die Schule wurde daher gebeten, die Kameras so auszurichten, dass die öffentliche Straße nicht mehr aufgezeichnet wird. Sollte dies nicht möglich sein, müsste geprüft werden, ob dieser Bereich bei den Aufnahmen jeweils ausgepixelt werden kann. Sollte die Schule den Forderungen des TLfDI nicht nachkommen, wird er – je nachdem, ob es sich um eine öffentliche oder eine nicht-öffentliche Stelle handelt – den Verstoß entweder beanstanden oder eine Anordnung nach § 38 Abs. 5 Satz 1 BDSG treffen.

Für die Handlungsmöglichkeiten des TLfDI ist es entscheidend, ob eine öffentliche oder eine nicht-öffentliche Stelle für die Datenverarbeitung verantwortlich ist. Für die Beurteilung von Videoaufzeichnungen kommt es bei einem sehr geringen Auflösungsgrad der Aufnahmen darauf an, ob die Personen, die sich im Aufnahmebereich der Kamera befinden, zumindest bestimmbar sind.

14.8 Handreichung zur Schulsozialarbeit

Mit dem Erlass der „Richtlinie über die Gewährung von Zuwendungen an örtliche Träger der öffentlichen Jugendhilfe für Vorhaben der schulbezogenen Jugendsozialarbeit vom 27. Mai 2013“ sind bis August 2015 über 260 Fachkräfte in den 23 Thüringer Landkreisen und kreisfreien Städten eingestellt worden. Für die Umsetzung der in der Richtlinie beschriebenen Ziele ist eine enge Kooperation mit den an der Schule tätigen Personen notwendig. Nach der Richtlinie sollen die individuellen und sozialen Kompetenzen der Kinder und Jugendlichen gefördert werden, soziale Benachteiligungen abgebaut und Lehrkräfte und Personensorgeberechtigte beraten werden. Vor dem Hintergrund eines präventiven Arbeitsansatzes sollte der Austausch zwischen den einzelnen Fachkräften (Lehrkräfte und schulbezogene Jugendsozialarbeiter) reibungslos funktionieren. Dabei ergaben sich jedoch zahlreiche datenschutzrechtliche Fragestellungen.
Da es in der Praxis immer wieder Fragen dazu gab, welche Daten unter welchen Voraussetzungen zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mehrere Schulungen zu diesem Thema für Schulleiter und Schulsozialarbeiter durch. Dabei ging es beispiels-

weise um die Fragen, welche Daten zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, ob Beratungen von Schülern trotz Verneinung durch die Personensorgeberechtigten durchgeführt werden dürfen oder wie lange Gesprächsakten aufzubewahren sind. Wichtig ist in diesem Zusammenhang vor allem, genau danach zu unterscheiden, wer personenbezogene Daten an wen übermittelt. Je nachdem gelten unterschiedliche Regelungen. Schulsozialarbeit als eine Aufgabe der Jugendhilfe wird ausschließlich nach den Regeln des Sozialgesetzbuches (SGB) erfüllt. Das Thüringer Schulgesetz regelt in § 57 Abs. 4 die Voraussetzungen der Übermittlung von personenbezogenen Daten an Dritte, zu denen auch die Schulsozialarbeiter gehören.
Dem TLfDI ist es aufgrund seiner knappen personellen Kapazität leider nicht möglich, alle von der Richtlinie Betroffenen zu schulen. Da die Inhalte der Schulung aber möglichst allen Betroffenen zur Verfügung stehen sollen, haben sich das Thüringer Ministerium für Bildung, Jugend und Sport als verantwortliches Ministerium sowie die fachliche Begleitung im entsprechenden Landesprogramm, die durch ein privates Unternehmen durchgeführt wird, dazu entschlossen, eine Handreichung zu dem Thema zu entwickeln. Grundlage war die vom TLfDI durchgeführte Schulung. Die Handreichung wurde inhaltlich mit dem TLfDI abgestimmt und wird im kommenden Berichtszeitraum als „Handreichung zum Datenschutz in der Schulsozialarbeit“ veröffentlicht. In diesem Dokument geht es neben den allgemeinen Regelungen und Begriffsklärungen insbesondere um die rechtliche Einordnung der Übermittlung von personenbezogenen Daten zwischen den Lehrkräften und den Schulsozialarbeitern beziehungsweise umgekehrt. Diese Bestimmungen werden in den einzelnen Kapiteln anhand von kleinen Fallbeispielen praktisch dargestellt.

Da für Schulsozialarbeiter das SGB gilt, für Schulen hingegen das Thüringer Schulgesetz, gestaltet sich die Beantwortung der Frage, welche Daten unter welchen Voraussetzungen zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, als nicht ganz einfach. Die Verantwortlichen haben gemeinsam mit dem TLfDI eine „Handreichung zum Datenschutz in der Schulsozialarbeit“ entwickelt, die Erläuterungen anhand von konkreten Fallbeispielen enthält.

14.9 Erhebung von personenbezogenen Daten im Kultusbereich – zur Integration erforderlich

Zur Fünften Verordnung zur Änderung der Thüringer Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich nahm auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Anfang des Jahres 2014 Stellung.
Die Thüringer Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich sollte mit Ablauf des 31. Juli 2014 außer Kraft treten. Für Zwecke der Bildungsplanung war von Seiten des ehemaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur (TMBWK) die Erhebung der Daten „Geburtsland (Staat); bei nichtdeutschem Geburtsland: Jahr des Zuzugs nach Deutschland; Staatsangehörigkeit; bei überwiegend nichtdeutscher Verkehrssprache in der Familie: Sprache bzw. Sprachengruppe“ über den 31. Juli 2014 hinaus erforderlich, da die erhobenen Daten die Grundlage für Meldungen an die Kultusministerkonferenz und das Statistische Bundesamt bilden würden. Zugleich war eine Ergänzung der bisher fehlenden Merkmale „Geburtsland und Jahr des Zuzugs nach Deutschland bei nichtdeutschem Geburtsland“ sowie „bei überwiegend nichtdeutscher Verkehrssprache in der Familie: Sprache“ entsprechend dem Beschluss der Kultusministerkonferenz zum „Kerndatensatz für schulstatistische Individualdaten der Länder“ notwendig. Bei diesen in Artikel 1 Nr. 1 des Verordnungsentwurfes ergänzten Merkmalen sollte demnach nur eine Lücke geschlossen werden, wie es bei der Mehrheit der Bundesländer bereits geschehen war.
Für den TLfDI war es noch fraglich, aus welchem Grund die Erhebung des Geburtslandes und die Erhebung des Jahres des Zuzugs nach Deutschland bei nichtdeutschem Geburtsland erforderlich seien. Das Ministerium teilte mit, dass im Rahmen der Beurteilung und der Analyse von Lernerfolgen beide Merkmale relevant seien. Aus dem Merkmal „Jahr des Zuzugs nach Deutschland“ könne die Verweildauer im deutschen Schulsystem ermittelt werden. Bei der statistischen Betrachtung, inwieweit das Schulsystem die Schüler zu einem bestimmten Abschluss führen kann, sei es durchaus von Bedeutung, ob bei den Migranten die Schullaufbahn überwiegend in Deutschland oder im Ausland absolviert wurde. Der Lernerfolg sei auch abhängig von der Verweildauer im deutschen Schulsystem. Bei

der genaueren statistischen Analyse der Migrantengruppen gäbe es große Unterschiede in den Lernerfolgen für verschiedene Herkunftsgebiete. Da viele Migranten bereits die deutsche Staatsbürgerschaft besäßen, sei das Merkmal „Geburtsland“ ein Merkmal zur Bestimmung der Unterschiede innerhalb der Migrantenpopulation. Diese Ausführungen sah der TLfDI als plausibel an.

Bei Verfahren zum Erlass bzw. Änderungen von Verordnungen, die datenschutzrechtliche Fragestellungen betreffen, ist auch der TLfDI einzubinden, damit sichergestellt ist, dass auch datenschutzrechtliche Belange hinreichend Berücksichtigung finden.

14.10 Anhörung zum Entwurf der Thüringer Fachschulordnung für die Bildungsgänge im Sozialwesen (ThürFSO-SW)

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Gelegenheit, zu dem in der Überschrift genannten Entwurf Stellung zu nehmen. Gegenüber dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) merkte er an, dass in dem Entwurf zwar die beim Antrag auf Aufnahme in die Fachschule einzureichenden Unterlagen im Einzelnen aufgelistet werden, nicht geregelt ist aber, wie mit diesen Unterlagen im Verlauf einer Ablehnung des Bewerbers durch die Fachschule umzugehen ist. Der TLfDI hat vorgeschlagen, in die Vorschrift eine Regelung aufzunehmen, wonach abgelehnte Bewerber die Unterlagen nach Abschluss des Aufnahmeverfahrens zurückerhalten. Ob dieser Vorschlag vom TMBJS berücksichtigt werden wird, ist bislang nicht bekannt, da der Entwurf sich derzeit noch in der Prüfung befindet und danach in den Bildungsausschuss zur Beratung überwiesen wird. Der TLfDI wird den weiteren Verlauf der Angelegenheit beobachten.

Um Irritationen hinsichtlich des weiteren Umgangs mit Antragsunterlagen im Zusammenhang mit dem Aufnahmeverfahren bei einer Fachschule zu vermeiden, sollte zusätzlich geregelt werden, wie mit solchen Unterlagen bei einer Ablehnung des Bewerbers umzugehen ist.

14.11 Kein Muster für Schulleistungsuntersuchungen

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erfolgte auf der Sitzung der Arbeitsgruppe Datenschutz und Schule am 16./17. September 2014 ein Meinungsaustausch über das Thema „Datenschutzrechtliche Prüfung bundeslandübergreifender Schulleistungsuntersuchungen“. Hintergrund hierfür war eine Anfrage des Deutschen Instituts für Internationale pädagogische Forschung bei den Landesbeauftragten für den Datenschutz (LfD), ob man das Verfahren der datenschutzrechtlichen Prüfung von wissenschaftlichen Bildungsforschungsvorhaben durch die LfD der jeweils an der Untersuchung teilnehmenden Bundesländer nicht vereinfachen könnte. So sollten Studienprojekte, die sich regelmäßig wiederholen, nur bei der ersten Genehmigung ausführlich geprüft werden. Als Ergebnis der Erörterung war festzustellen, dass eine abschließende Lösung der Problematik nicht erreicht werden konnte. Es bestehen Bedenken, pauschal dem Muster einer datenschutzrechtlichen Unbedenklichkeitserklärung gegenüber Schulleistungsuntersuchungen zuzustimmen. Dies insbesondere auch wegen der unterschiedlichen Rechtsvorschriften in den Ländern. In einigen Bundesländern, wie etwa auch in Thüringen, teilt der LfD seine datenschutzrechtliche Einschätzung zu einem Verfahren dem verantwortlichen Forschungsinstitut direkt mit, und das zuständige Thüringer Ministerium für Bildung, Jugend und Sport erteilt erst danach dem Institut die Genehmigung zur Durchführung der Untersuchung in den staatlichen Schulen. In anderen Bundesländern führt das jeweilige Kultusministerium die datenschutzrechtliche Prüfung des Verfahrens selbstständig durch und der zuständige LfD wird dann nur bei speziellen datenschutzrechtlichen Problemen beteiligt. Darüber hinaus können bei einzelnen datenschutzrechtlichen Fragestellungen durchaus unterschiedliche Rechtsauffassungen herrschen. Die Bildungsforscher schlugen auch vor, bei sich regelmäßig wiederholenden Projekten nur bei der erstmaligen Vorlage eine ausführliche datenschutzrechtliche Prüfung für die Prüfbehörde durchzuführen und bei nachfolgenden Genehmigungsverfahren geänderte oder neu eingefügte Sachverhalte entsprechend zu markieren, um auf diese Weise das Prüfverfahren abzukürzen. Fraglich ist aber, ob man sich tatsächlich auf solche Markierungen verlassen kann und die Forscher alle

von den LfD als erforderlich angesehenen Änderungen umgesetzt haben.

Schulleistungsuntersuchungen und andere Bildungsforschungsvorhaben, bei denen personenbezogene Schüler-, Eltern- und Lehrerdaten verarbeitet werden, müssen die Anforderungen der jeweiligen Datenschutzgesetze und anderer Rechtsvorschriften über den Datenschutz erfüllen. Für den Bereich der Thüringer Schulen hat der TLfDI gemäß § 37 Thüringer Datenschutzgesetz die Einhaltung dieser Bestimmungen zu kontrollieren.

14.12 Noten gehen nur die Betroffenen etwas an

Ein Schwarzes Brett findet sich in jeder Hochschule. Es birgt manchmal Gefahren für den Datenschutz. Hochschulangehörige baten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Mitteilung, unter welchen Voraussetzungen der öffentliche Aushang von Prüfungsergebnissen am Schwarzen Brett von Hochschulen und auch die Veröffentlichung solcher Ergebnislisten im Internet unter Nennung der Matrikelnummer sowie der dazugehörigen Note zulässig sind. Die Anfrage wurde zum Anlass genommen, alle Thüringer Hochschulen auf eine datenschutzgerechte Verfahrensweise bei der Veröffentlichung von Prüfungsergebnissen hinzuweisen. Prüfungsergebnisse, die einer konkreten Person zugeordnet werden können, sind personenbezogene Daten, deren Verarbeitung und Nutzung gemäß § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Durchsicht von einigen Hochschulsatzungen ergab, dass die Bekanntgabe von Noten unter Nennung der Matrikelnummer der betroffenen Studierenden dort als anonym bezeichnet wird. Grundsätzlich fallen anonyme Daten nicht mehr in den Anwendungsbereich des ThürDSG. Allerdings ist durchaus fraglich, ob die Matrikelnummer einen Personenbezug für Dritte praktisch tatsächlich ausschließt. Da Matrikelnummern in Verbindung mit den Namen der Studierenden innerhalb der Hochschule und auch außerhalb dieses Bereichs bei vielen Gelegenheiten Verwendung finden, etwa bei der Eintragung von Studierenden für eine Lehrveranstaltung, bei der Beantragung eines Login für einen Computerarbeitsplatz, bei der Beantragung eines Bibliothek-Benutzerkontos, bei der

Bearbeitung von Formularen in den BAföG- und Kindergeldstellen durch die Unterhaltspflichtigen sowie zum Nachweis der Studierendeneigenschaft gegenüber Verkehrsunternehmen, Zeitschriftenabonnements, Krankenversicherungen usw., ist ein Rückschluss auf eine bestimmte Person mit einer bestimmten Wahrscheinlichkeit durchaus möglich. Wenn Prüfungsergebnisse darüber hinaus nicht nur örtlich begrenzt am Schwarzen Brett des jeweiligen Fachbereichs, sondern auch zusätzlich im Internetauftritt der Hochschule, ohne persönliche Zugangsvoraussetzungen, etwa ein Login mit Nutzername und Passwort, veröffentlicht werden, so erweitert dies den Übermittlungsbereich (weltweit) beträchtlich. Der TLfDI hat den Hochschulen daher dringend empfohlen, die Studierenden bei der Aufnahme des Studiums darauf hinzuweisen, die Matrikelnummer Dritten gegenüber nicht bekanntzugeben. Weiterhin darf die Matrikelnummer von der Hochschule in keinem Zusammenhang mit personenidentifizierenden Merkmalen der Studierenden veröffentlicht werden. Ebenfalls darf eine Veröffentlichung von Prüfungsergebnissen mit Matrikelnummern im Internet ohne weitere Zugangsvoraussetzung nur dann erfolgen, wenn die Studierenden hierzu ausdrücklich ihre schriftliche Einwilligung erteilt haben. Die Hochschulen sollten Verfahren den Vorzug geben, bei denen z. B: durch Einrichten eines Benutzernamens mit Passwort sichergestellt ist, dass nur der Berechtigte auf seine Prüfungsergebnisse Zugriff hat. Eine datenschutzgerechte, wenn auch für die Hochschulen aufwendige Verfahrensweise liegt schließlich darin, für jede einzelne Prüfung einmalige, zufällig erzeugte Klausurnummern zu vergeben, die sich die Studierenden merken müssen, um das Prüfungsergebnis später bei der Veröffentlichung zuordnen zu können.

Matrikelnummern sind bei der Angabe in einem Aushang der Hochschule nur dann als ausreichend anonym anzusehen, wenn sie weder von den Studierenden noch von der Hochschule im Zusammenhang mit personenidentifizierenden Merkmalen des Betroffenen veröffentlicht werden. Eine Veröffentlichung von Prüfungsergebnissen unter Nennung der Matrikelnummer im Internet sollte von der Hochschule grundsätzlich nur in Form eines Logins mit Benutzername und Passwort erfolgen.

14.13 Tresen-Lösung im Prüfungsamt

In einer Eingabe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) beschwerte sich ein Student über die Organisation eines Prüfungsamtes der Hochschule. Auf Anfrage des TLfDI nach dem entsprechenden Sachverhalt, teilte die Hochschule mit, dass in diesem Prüfungsamt mehrere tausend Studierende mit ihren Prüfungen verwaltet werden. Man habe sich dort für eine als „Tresen-Lösung“ bezeichnete Organisation entschieden. Hierbei warten mehrere Studierende in einem Raum und werden durch Bedienstete des Prüfungsamtes an jeweils eine der nebeneinanderliegenden Bearbeitungsstellen gerufen, wobei diese lediglich durch einen kleinen Sichtschutz voneinander getrennt sind. Die Hochschule macht geltend, dass aufgrund der Einführung dieser Verfahrensweise die durchschnittlichen Wartezeiten der Studierenden von 90 Minuten auf etwa 10 Minuten reduziert werden konnten. Nach Angaben der Hochschule habe man die Anforderungen des Datenschutzes an die Wahrung der Vertraulichkeit bei einer solchen Lösung berücksichtigt und unter Beteiligung des behördlichen Datenschutzbeauftragten (bDSB) der Hochschule von Anfang an entsprechende Maßnahmen getroffen. Danach ist an der Eingangstür ein deutlich sichtbarer Hinweis angebracht, wonach Studierende, die für das Gespräch mit dem betreffenden Mitarbeiter oder der Mitarbeiterin Vertraulichkeit wünschen, dies zu Beginn des Gesprächs deutlich machen können, woraufhin der Mitarbeiter oder die Mitarbeiterin dann mit dem Studierenden das Gespräch in einem separaten Raum weiterführt. Diese Praxis habe sich bewährt, werde allerdings bislang selten von den Studierenden in Anspruch genommen. Dem beschwerdeführenden Studenten wurde vom TLfDI mitgeteilt, dass die gewählte Verfahrensweise aus datenschutzrechtlicher Sicht angesichts der hohen Zahl an Studierenden und des beschränkten Personal- und Platzangebotes sowie der gegebenen Möglichkeit, bei Bedarf vertrauliche Gespräche führen zu können, als akzeptabel anzusehen ist.

Auch bei der Durchführung von Massenverfahren an einer Hochschule haben die verantwortlichen Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die bestehenden datenschutzrechtlichen Bestimmungen zu gewährleisten.

Hochschulen müssen deshalb den Studierenden eine Möglichkeit einräumen, die Vertraulichkeit des Wortes zu wahren.

14.14 Betrugsverdacht bei Klausur – Einsicht in Smartphoneverläufe zulässig?

In einer anonymen Anfrage wandte sich ein Bürger mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob ein Dozent den Browserverlauf auf dem Smartphone eines Studierenden überprüfen darf. Hintergrund war ein Verdacht des Dozenten, dass der Student während einer Klausur unter Verwendung eines Smartphones einen Betrugsversuch unternommen hatte. Um diesen Verdacht zu widerlegen, forderte der Dozent noch in der laufenden Klausur beim Betroffenen die Herausgabe des Smartphones zur Offenlegung des Browserverlaufs, was der Student unter Verweis auf den Datenschutz ablehnte. Der TLfDI führte gegenüber dem Anfragenden aus, dass die vom Dozenten geforderte Einsicht in den Browserverlauf nur mit Einwilligung des Studenten erfolgen durfte. Da diese Einwilligung vom Betroffenen nicht erteilt wurde, bestand für den Dozenten keine Möglichkeit, den Browserverlauf durchzusehen, denn es gibt keine Befugnisnorm für Dozenten oder Lehrer zur Beschlagnahme und zum Auslesen eines Handys. Gegen den Willen des Betroffenen dürfen daher Inhalte auf Smartphones nicht ausgewertet werden. Im Rahmen der datenschutzrechtlichen Grundsätze von Datenvermeidung und Datensparsamkeit hätte der Dozent auch mit Einwilligung des Betroffenen lediglich Einsicht in den die prüfungsrelevante Zeit betreffenden Teil des Browserverlaufs nehmen dürfen. Welche Konsequenzen sich aber für den Studenten aus der nicht erteilten Einwilligung ergaben, entzog sich der datenschutzrechtlichen Beurteilung. Um solche Konflikte bei der Nachweisführung von Täuschungsversuchen zu verhindern, haben viele Schulen und Hochschulen in ihren Prüfungsordnungen oder schulinternen Ordnungen festgelegt, dass bei förmlichen Prüfungen bereits ein mitgeführtes Handy bzw. Smartphone als Täuschungsversuch gewertet werden kann.

Handys bzw. Smartphones von Studierenden und Schülern dürfen von Lehrkräften nicht ohne Einwilligung des Betroffenen eingesehen werden. Um Konflikte von vornherein auszuschließen, bietet es sich an, in Prüfungsordnungen und internen Schulordnungen zu regeln,

dass zur Prüfung keine eingeschalteten Handys bzw. Smartphones mitgeführt werden dürfen.

14.15 E-Mail zwischen Schule und Schulamt

In einer Eingabe wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass zwischen den Schulen und dem zuständigen staatlichen Schulamt regelmäßig personenbezogene Schuldaten im unverschlüsselten E-Mail-Verkehr übermittelt wurden. Es handelte sich um Schülerdaten, etwa sonderpädagogische Gutachten, Aufnahmeanträge von Schülern, Daten der Personalplanung der Lehrer sowie dienstliche Beurteilungen von Lehrkräften. Der TLfDI wandte sich mit dieser Problematik an das damalige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) und wies dort auf die Regelungen des § 9 Thüringer Datenschutzgesetz (ThürDSG) hin, wonach öffentliche Stellen bei der Verarbeitung personenbezogener Daten die erforderlichen technischen und organisatorischen Maßnahmen zu treffen haben, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Eine Übermittlung personenbezogener Daten mit einer E-Mail kann die Vertraulichkeit und Integrität der übermittelten personenbezogenen Daten nicht gewährleisten. Der E-Mail-Inhalt kann von Dritten mitgelesen oder sogar verändert bzw. verfälscht werden. Daher sind Texte, die personenbezogene Daten enthalten, vom Absender zu verschlüsseln. Die verschlüsselten Texte müssen dann vom Empfänger entschlüsselt, also in den Klartext zurückverwandelt werden. Das TMBWK teilte dem TLfDI in einer Stellungnahme mit, dass für die Übermittlung personenbezogener Daten zwischen den Schulen, Schulämtern und dem Ministerium innerhalb der Verwaltungsplattform Schulwesen (THVPS) ein Austauschserver eingerichtet wurde. Dokumente, die hierüber übermittelt werden, unterliegen einer dreifachen Sicherung des THVPS, nämlich in Form einer PIN, einer Autorisierungskarte und einem eineindeutigen Authentifizierungstoken. Wer keinen Zugriff auf das THVPS besitzt, soll die Papierform verwenden. Das TMBWK hatte dem TLfDI zugesagt, bei einer Schulamtsleiterberatung die Problematik zu thematisieren und dort darum zu bitten, dies auch an die Schulleiter weiterzugeben. Der TLfDI teilte dem TMBWK mit, dass aus datenschutzrechtlicher Sicht keine Bedenken gegen die Verwendung des THVPS bestehen und hat angeregt, an die Problematik des

Versands von personenbezogenen Daten per E-Mail regelmäßig in Beratungen mit den Schulamtsleitern zu erinnern.

Personenbezogene Daten dürfen per E-Mail zwischen öffentlichen Stellen, im vorliegenden Fall zwischen Schule und Schulamt, nur übermittelt werden, wenn ein anerkanntes Verschlüsselungsverfahren eingesetzt wird. Andernfalls stellt die unverschlüsselte Übermittlung einen Verstoß gegen die Regelungen des § 9 ThürDSG dar.

14.16 Fakten, Fakten, Fakten: www.youngdata.de – nicht nur für Jugendliche!

Am 10. Februar 2015 wurde im Rahmen einer Veranstaltung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zum Safer Internet Day mit dem Thema „Medienkunde als eigenes Schulfach – Neuland in Sicht?“ per symbolischem Knopfdruck der Startschuss für das gemeinsame Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes und der Länder http://www.youngdata.de/ gegeben, wobei der Start der Seite große Resonanz in den Medien fand. Mit diesem Internetauftritt wollen die Datenschutzbeauftragten die Aufmerksamkeit von Kindern und Jugendlichen für die Themen Datenschutz und Datensicherheit stärken und gegen mangelndes Wissen in diesen Bereichen vorgehen. Das Portal bietet dabei aktuelle Datenschutz-Nachrichten, Videos, Cartoons, Quiz und Tipps, wie man seine Daten am besten schützen kann. Die Betreuung der verschiedenen Hauptmenüpunkte haben die Datenschutzbeauftragten der Länder unter sich aufgeteilt. Der TLfDI hat dabei die inhaltliche Pflege und Betreuung der Hauptmenüpunkte „Videoüberwachung“ und „Informationsfreiheit“ übernommen. Unter einem weiteren Hauptmenüpunkt „Was gibt’s in deiner Nähe?“ haben alle Datenschutzbeauftragten die Möglichkeit, auf jeweils eigene Bildungs- und Informationsangebote hinzuweisen. Inzwischen wurde das Portal durch jugendspezifische Angebote zum Thema „Selbstdatenschutz“ unter dem Menüpunkt „Digitale Selbstverteidigung“ erweitert. Hierin werden konkrete Tipps gegeben, was Jugendliche tun können, um ihre Daten besser zu schützen, z. B. in

einem sozialen Netzwerk, bei der Nutzung eines Messenger-Dienstes oder auf dem eigenen Smartphone.
Zutritt zur Seite haben natürlich auch Erwachsene ;-)

Mit http://www.youngdata.de/ haben die Datenschutzbeauftragten des Bundes und der Länder ein gemeinsames Internetportal geschaffen, das sich besonders an Kinder und Jugendliche richtet und Informationen zum Datenschutz, zur Datensicherheit und zur Informationsfreiheit gibt.

14.17 Hänseleien bei der Bekanntgabe von Schulnoten vor der Klasse

Die Mutter eines 11-jährigen Schulkindes wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und berichtete von einigen Lehrkräften, die bei Schülerinnen und Schülern im Unterricht anfragten, ob diese in die Bekanntgabe ihrer Endjahresnote vor der Klasse einwilligen. Bei dem Schulkind im vorliegenden Fall wurden nach dessen Zustimmung die durchweg sehr guten Noten angesagt. Dies hatte zur Folge, dass das Kind nunmehr den Hänseleien der anderen Schülerinnen und Schüler ausgesetzt war und von diesen auch ausgegrenzt wurde. Die Mutter bat den TLfDI daraufhin um Aufklärung, unter welchen Voraussetzungen Zensuren vor der Klasse mitgeteilt werden dürfen und ob sie aufgrund ihrer Erfahrung die öffentliche Bekanntgabe der Noten ihres Kindes verhindern kann. Der TLfDI legte der Beschwerdeführerin dar, dass es sich bei Schulnoten aus datenschutzrechtlicher Sicht um personenbezogene Daten im Sinne von § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) handelt. Die Bekanntgabe von Schulnoten vor der Klasse stellt eine Übermittlung personenbezogener Daten an Dritte dar und ist somit nach § 3 Abs. 3 ThürDSG eine Verarbeitung personenbezogener Daten. Das Verarbeiten und Nutzen personenbezogener Daten ist gemäß § 4 Abs. 1 ThürDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die spezialgesetzliche Regelung des Thüringer Schulgesetzes (ThürSchulG) führt in § 57 Abs. 4 Nr. 3 aus, dass eine Übermittlung personenbezogener Daten an Dritte nur zulässig ist, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Darüber hinaus bestimmt § 57 Abs. 1 ThürSchulG, dass das Verarbeiten und Nutzen

personenbezogener Daten der Schüler zur Erfüllung der den Schulen zugewiesenen Aufgaben zulässig ist, soweit dies für den jeweils mit den Aufgaben verbundenen Zweck erforderlich ist. Ob die Bekanntgabe von (Zeugnis-)Noten im Unterricht überhaupt zulässig ist, muss aus pädagogischer Sicht beurteilt werden. Gemäß § 48 Abs. 3 ThürSchulG ist die Transparenz der Notengebung für Schüler und Eltern zu gewährleisten. Fraglich ist allerdings, ob die Transparenz der Notengebung personenbezogen erfolgen darf oder aber, ob hierfür nicht ein anonymer Notenspiegel diese Aufgabe ausreichend erfüllt. Soweit eine Schule die Notenbekanntgabe vor der Klasse aus pädagogischer Sicht für sinnvoll erachtet, kann dies aus datenschutzrechtlicher Sicht ausschließlich auf der Grundlage einer rechtswirksamen Einwilligung der Betroffenen erfolgen. Voraussetzung für eine wirksame Einwilligung ist, dass der Schüler die Tragweite seiner Entscheidung überblicken kann. Verbindliche Altersgrenzen für die Erteilung einer Einwilligungserklärung gibt es somit nicht. Der TLfDI geht aber davon aus, dass ein 11-jähriges Kind nur in den wenigsten Fällen selbst genügend Einsichtsfähigkeit hat, um eine verbindliche Einwilligungserklärung selbst abgeben zu können. Als grober Anhaltspunkt ist hier je nach vorliegendem Sachverhalt zumindest das 14. Lebensjahr anzusehen. In Zweifelsfällen sollte die Schule daher die Einwilligung der Eltern einholen.
Da die Mutter im vorliegenden Fall die Schule nicht benannte, konnte der TLfDI nicht tätig werden.

Die schulgesetzlichen Bestimmungen enthalten keine Regelung zur Bekanntgabe von Zeugnisnoten vor der Klasse. Wird dies aus pädagogischen Gründen für erforderlich gehalten, ist dies nur auf der Grundlage einer Einwilligung zulässig. Die Erteilung einer rechtswirksamen Einwilligung erfordert eine entsprechende Einsichtsfähigkeit der Schülerinnen und Schüler. Hierfür gibt es keine starre Altersgrenze, in Zweifelsfällen sollte jedoch der Elternwille beachtet und die Eltern um die Einwilligung ersucht werden.

14.18 Lehrkräfte führen privates Girokonto zu Schulzwecken?

Aufgrund der Anfrage eines anderen Landesdatenschutzbeauftragten wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darüber informiert, dass es in Schulen dort üblich sei, dass Lehrkräfte im Zusammenhang mit der fiskali-

schen Abwicklung von zum Beispiel Klassenfahrten für diese Zwecke ein Privatkonto eröffnen. Hier sind auch datenschutzrechtliche Aspekte berührt, etwa bei der Datenerhebung durch die Banken bei der Kontoeröffnung und einer möglichen Übermittlung personenbezogener Daten an die Schufa oder die Erhebung personenbezogener Daten Dritter, die als zusätzliche Verfügungsberechtigte eingetragen werden. Der TLfDI nahm den geschilderten Sachverhalt zum Anlass, sich an das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) zu wenden und nachzufragen, ob auch in Thüringen Privatkonten von Lehrkräften zu schulischen Zwecken geführt werden. In seiner Antwort wies das TMBJS darauf hin, dass es einen Entwurf einer Verwaltungsvorschrift zur Einrichtung und Führung von Schulkonten erarbeitet hatte, hierzu aber Dissens zur Frage entstand, ob diese Konten in der Inhaberschaft der Schulträger oder aber des Landes Thüringen zu führen seien. Bis zum gegenwärtigen Zeitpunkt konnte keine Klärung erreicht werden, ob die Kontoinhaberschaft für Girokonten der Schulen beim Land oder bei den Schulträgern liegt. Das TMBJS stimmte dem TLfDI zu, dass Kontoinhaberschaften durch Lehrkräfte als Privatpersonen auf keinen Fall vorgesehen sind. Der TLfDI wird weiterhin beobachten, wann eine Verwaltungsvorschrift die Einrichtung und Führung von Schulkonten regelt. Offenbar ist aber in Thüringen kein flächendeckender Handlungsbedarf in der Frage gegeben.

Die Eröffnung und Führung von Privatkonten durch Lehrkräfte zu schulischen Zwecken ist aus datenschutzrechtlicher Sicht bedenklich. Das Land hat dafür Sorge zu tragen, dass bei Zahlungsverkehr für schulische Angelegenheiten keine privaten Konten zum Einsatz kommen.

14.19 Schülerdaten im Netz

Besorgte Eltern berichteten dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von einer im Internet ohne weitere Zugangsvoraussetzungen zugänglichen Excel-Tabelle, in der die Namen, die Adressen und Telefonnummern aller Schülerinnen und Schüler einer Grundschule sowie die Namen der Elternteile, teilweise mit entsprechenden Hinweisen auf die Sorgeberechtigten, enthalten waren. Der TLfDI wandte sich umgehend an die Schule mit der Forderung, die Seite unverzüglich aus dem Inter-

net zu entfernen. Aus datenschutzrechtlicher Sicht liegt in einer Internetveröffentlichung von Schüler- und Elterndaten eine weltweite Datenübermittlung. Eine solche Übermittlung personenbezogener Daten im Internet ist nur dann zulässig, wenn eine der in § 23 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) aufgeführten Voraussetzungen vorliegt, was in diesem Fall nicht ersichtlich war. Wie die Schule in ihrer Stellungnahme mitteilte, war die Seite völlig unbeabsichtigt im Thüringer Schulportal veröffentlicht worden. Das Thüringer Schulportal ist eine Arbeitsplattform für den Kultusbereich in Thüringen, die zum Beispiel Schulporträts, Neuigkeiten aus der Bildungslandschaft Thüringen, Unterrichtsmaterialien für Lehrkräfte usw. veröffentlicht. Nach Angaben der Schulleiterin war die eigentliche Absicht, die Klassenlisten für Zwecke des Krisenmanagements nach § 136 Abs. 10 der Thüringer Schulordnung in das Schulportal zu übertragen. Hierbei besteht eine Zugriffsmöglichkeit nur seitens des zuständigen Schulamts. Ein Zugriff ist nur im Falle von Krisen- oder Notfällen zulässig. Aus für die Schulleiterin unerklärlichen Gründen sei ihr bei der Übermittlung an das Portal offenbar ein Fehler unterlaufen. Sie bedauerte den Vorfall und sagte dem TLfDI zu, in Zukunft noch genauer auf korrekte Datenübertragungen von personenbezogenen Daten zu achten. Noch während der Klärung des Sachverhalts konnte der TLfDI feststellen, dass die Schülerliste nicht mehr im Internet öffentlich abrufbar war. Der TLfDI hatte in dem vorliegenden Fall von einer Beanstandung abgesehen, da die Schule den Fehler eingeräumt hatte, der Mangel sofort beseitigt wurde und eine noch sorgfältigere Beachtung der datenschutzrechtlichen Vorschriften versichert wurde.

Die Schule hat bei der Verarbeitung von personenbezogenen Schüler- und Elterndaten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen des ThürDSG zu gewährleisten (§ 9 Abs. 1 ThürDSG). Der TLfDI kann nach § 39 Abs. 4 ThürDSG von einer Beanstandung absehen, insbesondere wenn es sich um inzwischen beseitigte Mängel handelt.

14.20 Soziale Netzwerke in der Ausbildung im Vorbereitungsdienst für die Lehrämter

Das für die Lehrerausbildung ehemals zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung einer Community-Plattform, die ein Seminarschulverbund einführen wollte. Die Plattform sollte als Kommunikationsmedium über das Internet zwischen den Fachleitern und den Lehramtsanwärtern dienen. Hiermit sollte diesem Personenkreis ein Zugang zu Lerninhalten und -angeboten sowie der Austausch von Materialien ermöglicht werden. Der TLfDI teilte im Ergebnis die im TMBWK bereits bestehenden Bedenken gegen die Nutzung der Community-Plattform. Nach wie vor rät der TLfDI von der Nutzung vieler angebotener sozialer Netzwerke zur Aufgabenerfüllung öffentlicher Stellen im Hinblick darauf ab, dass die meisten Anbieter und Betreiber in der USA ansässig sind und nunmehr amtlich ist, dass das Safe-Harbor-Abkommen zum Schutz personenbezogener Daten den datenschutzrechtlichen Anforderungen in der Europäischen Union nicht gerecht geworden ist (vgl. Urteil des EuGH vom 6. Oktober 2015). Im vorliegenden Fall war insbesondere die Nutzung der Online-Plattform über Drittanbieter, z. B. Facebook oder Twitter, kritisch anzusehen. Die Plattform sah eine Verknüpfung mit anderen sozialen Netzwerken in der Form vor, dass man sich auch über diese Drittanbieter in die Plattform einloggen konnte. Somit war nicht auszuschließen, dass zumindest beim Login Daten an das gewählte soziale Netzwerk dieses Drittanbieters übertragen werden. Der Seminarschulverbund schlug deshalb vor, die Nutzung der Plattform auf der Grundlage einer Einwilligung durch die Teilnehmer zu ermöglichen. Da der Einsatz dieses Verfahrens zwar dienstlich nicht vorgeschrieben werden sollte, den Lehramtsanwärtern jedoch nach dem geplanten Konzept mit Einstieg in den Vorbereitungsdienst zur Nutzung als Mittel zur Ausbildung angeboten wurde, hätte die Verantwortung für die datenschutzgerechte Verarbeitung und Nutzung der Daten auf der Community-Plattform allein beim Seminarschulverbund und nicht beim einzelnen Nutzer gelegen. Der TLfDI wies weiter darauf hin, dass der Seminarschulverbund als verantwortliche Stelle mit dem die Online-Plattform anbietenden Unternehmen einen Vertrag über eine Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG)

abschließen müsse. Die verantwortliche Stelle als Auftraggeber hat beim Auftragnehmer die von diesem getroffenen technischen und organisatorischen Maßnahmen zu prüfen. Auch hiernach wäre der Hochschulverbund für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich geblieben. Nach Kenntnissen des TLfDI wurde der Einsatz der Online-Plattform durch den Seminarschulverbund nicht weiter verfolgt.

Bei der Nutzung einer Online-Plattform eines externen Dienstleisters hat die verantwortliche Stelle zu prüfen, ob dieser die datenschutzrechtlichen Anforderungen erfüllt. Die verantwortliche Stelle muss „Herrin der Daten“ bleiben. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht hinsichtlich der Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen.

14.21 Weltweite Veröffentlichung von Schülernamen und Abiturprüfungszeiten

In der Eingabe eines Schülers beschwerte dieser sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Veröffentlichung von Prüfungszeiten für das mündliche Abitur im Internetauftritt einer Schule. Man erhielt auf dieser Seite Einblick in eine Liste, aus der ersichtlich war, welcher Prüfling mit Namen und Vornamen an welchem Tag zu welcher Zeit und in welchem Fach mündlich geprüft wurde. Die weitere Durchsicht der Schulhomepage ergab, dass die Stundenpläne aller Schulklassen unter Nennung des Namens der Klassenlehrer/innen sowie die entsprechenden Klassenfotos eingestellt waren. Weiterhin waren Vertretungspläne abrufbar, in denen unter Angabe der jeweiligen Klasse und des Fachs ersichtlich war, durch welche Lehrkraft ein abwesender Lehrer vertreten wird. Der TLfDI schrieb die Schule an und wies darauf hin, dass eine namensbezogene Veröffentlichung von Prüfungslisten und Vertretungsplänen im Internet eine weltweite Übermittlung personenbezogener Daten darstelle, die nicht zur Aufgabenerfüllung der Schule erforderlich sei. Nach § 57 Abs. 4 Thüringer Schulgesetz (ThürSchulG) ist eine Übermittlung personenbezogener Daten an Dritte nur unter den dort genannten Voraussetzungen zulässig. Eine dieser Voraussetzungen ist die Einwilligung durch die Betroffenen. Da nach § 4 Abs. 1 Satz 2 Thüringer Datenschutzgesetz

(ThürDSG) eine Verarbeitung und Nutzung personenbezogener Daten mit Einwilligung der Betroffenen nur dann zulässig ist, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist, war bereits aus diesem Grund die Zulässigkeit der Datenveröffentlichungen im Internet fraglich. Insbesondere ist die Zulässigkeit einer Veröffentlichung personenbezogener Daten mit Einwilligung durch die Lehrkräfte zweifelhaft, da aufgrund des Beschäftigtenverhältnisses der Lehrkräfte mit der Daten verarbeitenden Stelle ein Abhängigkeitsverhältnis besteht und daher nicht von einer freiwilligen Einwilligung ausgegangen werden kann. Zur Veröffentlichung von Klassenfotos verwies der TLfDI auf § 56 Abs. 1 Satz 6 Thüringer Schulgesetz, wonach die Mitwirkung an Klassenfotos freiwillig ist. Nach § 4 ThürDSG ist eine Verarbeitung und Nutzung der personenbezogenen Daten nur zulässig, wenn der Betroffene (hier Schüler/in) bzw. die Erziehungsberechtigten eingewilligt haben. Die Einwilligung bedarf der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 4 Abs. 3 Satz 2 ThürDSG). Die Schulleitung erläuterte, dass eine Veröffentlichung von Prüfungslisten für das mündliche Abitur ein Ausnahmefall wäre, der einer besonderen schulischen Situation geschuldet gewesen sein soll und in vorheriger mündlicher Absprache mit den Schülern erfolgt sei. Die Schule sagte zu, solche Listen zukünftig nicht mehr zu veröffentlichen. Hinsichtlich der Veröffentlichung von Klassen- und Schülerfotos gab die Schule an, jährlich eine Fotoerlaubnis schriftlich bei allen Eltern einzuholen. Bei der Veröffentlichung von Namen der Lehrkräfte im Vertretungsplan sei diese nach einem Schreiben aus dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur vom 21. März 2010 an die staatlichen Schulämter durch Einholung einer rechtswirksamen Einwilligung bei den Lehrkräften zulässig. Den Lehrkräften sei auch das Recht eingeräumt worden, die Einwilligung jederzeit schriftlich zu widerrufen. Die Schulleitung sagte dem TLfDI aber zu, zukünftig auf die Nennung der Nachnamen zu verzichten und nur noch Kürzel zu verwenden. Da der TLfDI bei der Durchsicht des Internetauftritts feststellen musste, dass die Liste der mündlichen Abiturkandidaten noch immer abrufbar war, wurde die Schule erneut aufgefordert, die Seite unverzüglich zu entfernen und dem TLfDI das hierzu Veranlasste mitzuteilen. Dies wurde daraufhin von der Schule erledigt.

Bei der Veröffentlichung personenbezogener Daten auf der Schulhomepage hat die Schule als verantwortliche Stelle vorab zu prüfen, ob dies zulässig ist. Im Regelfall müssen die Betroffenen vor der Veröffentlichung ihrer Daten im Internet von der Schule um eine schriftliche Einwilligung ersucht werden. Bei der Veröffentlichung von Vertretungsplänen dürfen keine Namen der vertretenen oder der vertretenden Lehrkräfte genannt werden. Idealerweise sind auch Kürzel so zu wählen, dass diese für Dritte außerhalb der Schule nicht personenbeziehbar sind.

14.22 Elektronisches Klassenbuch: datenschutzrechtlich nicht ohne

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten einige Anfragen zur Nutzung des elektronischen Klassebuchs in staatlichen Schulen des Freistaats Thüringen. Dabei erfolgten die bisherigen Anfragen nicht seitens der Schulen oder Schulaufsichtsbehörden, sondern von den Schulverwaltungsämtern, also den kommunalen Schulträgern, die unter anderem den für den Schulbetrieb und Unterricht erforderlichen Sachaufwand tragen (§ 3 Abs. 2 Thüringer Gesetz über die Finanzierung der staatlichen Schulen). Hierzu gehört auch die Beschaffung und Finanzierung der in der Schule verwendeten Soft- und Hardware und damit auch die Einführung des elektronischen Klassenbuchs. Hierunter ist eine Software zu verstehen, die die Führung des herkömmlichen Klassenbuchs in Papierform ergänzen oder ersetzen soll. Dabei gehen die Möglichkeiten des elektronischen Klassenbuchs weit über die Funktionen des bisherigen Klassenbuchs hinaus. Es können viel mehr Angaben als bisher erhoben werden.
Welche personenbezogenen Schüler- und Elterndaten zu welchen Zwecken verarbeitet werden dürfen, ist aber in § 136 Abs. 4 und 10 der Thüringer Schulordnung abschließend geregelt. Somit darf die Schule alle anderen Funktionen der Software nicht nutzen und muss diese deaktivieren. Darüber hinaus werden beim elektronischen Klassenbuch die personenbezogenen Daten im Regelfall nicht von der Schule selbst oder einer staatlichen Stelle, sondern bei einem privaten Dritten oder in einer Cloud in Auftragsdatenverarbeitung gemäß § 8 Thüringer Datenschutzgesetz gespeichert. Deshalb muss die Schule bzw. ein staatliches Schulamt eine Vereinbarung über die Verarbeitung der personenbezogenen Daten mit dem Anbieter des

elektronischen Klassenbuchs schließen. Sowohl der Speicherplatz als auch der Übertragungsweg vom Schulrechner auf den Speicher bedürfen einer vorherigen ausführlichen datenschutzrechtlichen Prüfung. Genau diese Problematik war dem Hinweis eines Schulverwaltungsamtes zu entnehmen, wonach dort angedacht war, die Daten in einer Cloud zu speichern und den Lehrkräften der jeweiligen Klasse einen lesenden und schreibenden Zugriff einzurichten. Auch den Eltern der Schülerinnen und Schüler sollte über ein Login ein lesender Zugriff ermöglicht werden, damit sie sich über An- und Abwesenheiten vom Unterricht ihres Kindes, Fehlzeiten, Klassenbucheinträge, Prüfungen etc. auf elektronischem Wege informieren konnten. Das Schulverwaltungsamt gab dabei an, für die datenschutzrechtliche und die datensicherheitstechnische Zulässigkeit des Verfahrens keine Verantwortung tragen zu können. Die Verantwortung für den Umgang mit Schüler-, Lehrer- und Elterndaten zu schulischen Zwecken liege bei der Schule bzw. bei den Schulaufsichtsbehörden. Diese Auffassung teilt der TLfDI bereits seit Längerem und stand hierzu bereits mit dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur in Kontakt. Eine vollständige Klärung des Sachverhalts steht noch aus. Zum konkreten Sachverhalt teilte das zuständige staatliche Schulamt mit, dass es sich lediglich um schulinterne Vorüberlegungen handele und Informationen gesammelt werden sollten. Der TLfDI hatte das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) gebeten, aufzulisten, wie viele staatliche Schulen in Thüringen ein elektronisches Klassenbuch nutzen. Inzwischen hat das Ministerium eine solche Liste, basierend auf den Rückmeldungen der Schulen, an den TLfDI übersandt. Danach nutzen erst ca. 100 Schulen ein elektronisches Klassenbuch. Die nähere Auswertung der dabei genutzten Systeme muss noch erfolgen. Der TLfDI bleibt in der Sache am Ball und wird die zukünftige Entwicklung verfolgen. Er hat das TMBJS gebeten, alle Schulen auf die Rechtslage hinzuweisen, dass die Funktionen der Software nicht genutzt werden dürfen, die die Anforderungen des § 136 Abs. 4 und 10 der Thüringer Schulordnung nicht erfüllen.

Nicht alles, was das elektronische Klassenbuch kann, darf von der Schule auch genutzt werden. Bei Dateninhalten und Zugriffsregelungen müssen die gesetzlichen Regelungen, die für das herkömmliche Klassenbuch in Papierform gemäß § 136 Abs. 4 und 10 Thüringer Schulordnung gelten, gleichfalls beachtet werden.

14.23 Alte Klassenbücher: Oldies sind datenschutzrechtlich keine Goldies

Aus Anlass des 50-jährigen Schulabschlusses wollten einige der Ehemaligen in den alten Klassenbüchern stöbern, um in geselliger Runde den einen oder anderen Klassenbucheintrag zum Besten zu geben. In diesem Zusammenhang brachte eine Beschwerdeführerin gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ihre Empörung zum Ausdruck, dass einige Schulen sich geweigert hatten, die Einsicht in die mindestens 50 Jahre alten Klassenbücher zuzulassen. Die Bürgerin war der Auffassung, dass so alte Daten in den Klassenbüchern unmöglich noch schützenswert sein können. So sehr der Unterhaltungswert von alten Klassenbucheinträgen nachvollziehbar ist, musste der TLfDI der Beschwerdeführerin mitteilen, dass auch personenbezogene Daten in 50 Jahre alten Klassenbüchern personenbezogene Daten bleiben. Auch in diesen Fällen darf eine Schule nach § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz personenbezogene Daten an Dritte nur dann übermitteln, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Auch das Thüringer Schulgesetz erlaubt in § 57 Abs. 4 Nr. 3 die Übermittlung personenbezogener Daten an Dritte nur, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Eine Einsichtnahme in diese Klassenbücher wäre demnach lediglich auf der Grundlage einer Einwilligung aller noch lebenden ehemaligen Schülerinnen und Schüler zulässig gewesen. Darüber hinaus war der TLfDI davon überrascht, dass eine Schule noch Klassenbücher aufbewahrte, die vor 50 Jahren ihren Abschluss gefunden hatten. Nach § 136 Abs. 8 Thüringer Schulordnung sind personenbezogene Daten in nicht automatisierten Dateien und Akten nach Maßgabe der hierfür geltenden Bestimmungen aufzubewahren und nach Ablauf der jeweiligen Frist zu vernichten oder zu archivieren. In Thüringen ist nach einem Schreiben des ehemaligen Thüringer Kultusministeriums vom 24. Juni 2014 für Klassenbücher eine Aufbewahrungsfrist von 2 Jahren vorgesehen. Diese sind danach den örtlichen bzw. kreislichen Archiven anzubieten. Da dem TLfDI der Name der Schule nicht bekannt geworden war, konnte er die Schule nicht auf die entsprechende Regelung hinweisen.

Auch auf personenbezogene Daten von Schülerinnen und Schülern in alten Klassenbüchern finden datenschutzrechtliche Regelungen Anwendung. Ohne eine spezielle Rechtsvorschrift, die eine Übermittlung dieser Daten an Dritte erlaubt, kann sich die Zulässigkeit der Übermittlung nur aus einer rechtswirksamen Einwilligung ergeben. Die Schulen sind angehalten, ihren Datenbestand laufend daraufhin zu überprüfen, ob Aufbewahrungsfristen abgelaufen sind und die Unterlagen dem zuständigen Archiv angeboten oder vernichtet werden müssen.

14.24 BAföG21, Dialog21 und Kasse21

Das Bundesausbildungsförderungsgesetz (BAföG) regelt die staatliche Unterstützung für die Ausbildung von Schülern und Studenten. Mit dem Ziel, das Verfahren der Erhebung personenbezogener Daten beim Antragsteller bis zur Prüfung, Berechnung und Auszahlung der Förderleistung zu beschleunigen, hat der Freistaat Thüringen die Verfahren BAföG21, Dialog21 und Kasse21 eingeführt. In den meisten anderen Bundesländern werden diese automatisierten Verfahren ebenfalls genutzt. Es wird seit dem Jahr 2014 in Thüringen eingesetzt. Es handelt sich um eine Modernisierung der vormals bestehenden IT-Verfahren. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat das neue Verfahren aus datenschutzrechtlicher Sicht begleitet und war bereits im Jahr 2009 hiermit beschäftigt. Der Verfahrensgang stellt sich so dar, dass zunächst die Beantragung von Leistungen nach dem BAföG in dem Amt für Ausbildungsförderung bei den kreisfreien Städten und den Landkreisen sowie beim Studentenwerk Thüringen an den Hochschulstandorten erfolgt. Die dort erhobenen Daten des Antragstellers werden dann in einem zentralen Hauptverfahren im Thüringer Landesrechenzentrum im Auftrag des damaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur (TMBWK) und jetzigen Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) weiterverarbeitet. In diesem Hauptverfahren erfolgen eine Plausibilitätsprüfung, die Berechnung der Förderleistung, die Bescheiderstellung und die Zahlungsanweisung. Der TLfDI prüfte zunächst den Entwurf des für das Verfahren erstellten Sicherheitskonzepts. Der im Ergebnis erforderliche Ergänzung- und Änderungsbedarf wurde vom Thüringer Landesrechenzentrum im Auftrag des TMBWK in das Sicherheitskonzept eingear-

beitet. Die Forderungen in diesem zentral erstellten Sicherheitskonzept müssen von allen beteiligten Thüringer Ämtern für Ausbildungsförderung umgesetzt und das Verfahren von den Ämtern als Daten verarbeitende Stellen nach § 10 Thüringer Datenschutzgesetz(ThürDSG) in das Verfahrensverzeichnis aufgenommen werden. Die Freigabe des Verfahrens nach § 34 Abs. 2 ThürDSG erfolgte für alle Ämter für Ausbildung zentral seitens des TMWWDG, das jedoch keinen Zugriff auf die verarbeiteten Daten der Antragsteller hatte.

Seit dem Jahr 2014 werden die personenbezogenen Daten der Antragsteller und Bezieher von Förderleistungen nach dem BAföG mit den Verfahren BAföG21, Dialog21 und Kasse21 verarbeitet. Nach Prüfung des TLfDI bestehen gegen den Einsatz nach derzeitigen Erkenntnissen keine datenschutzrechtlichen Bedenken.

14.25 Novellierung des Thüringer Gesetzes über Schulen in freier Trägerschaft

Im Rahmen der geplanten Novellierung des Thüringer Gesetzes über Schulen in freier Trägerschaft (ThürSchfTG) bat das damalige Thüringer Ministerium für Bildung, Wissenschaft und Kultur den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft und Stellungnahme zu einem möglichen Widerspruch zwischen der Regelung des § 5 Abs. 10 Satz 4 ThürSchfTG und der Bestimmung des § 72a Abs. 5 Sozialgesetzbuch (SGB) Achtes Buch (VIII). Konkret stellt sich die Rechtslage so dar, dass nach § 72a Abs. 5 SGB VIII die Träger der öffentlichen und freien Jugendhilfe für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Personen beschäftigen oder vermitteln dürfen, die rechtskräftig wegen einer Straftat im Zusammenhang mit Kindern und Jugendlichen (z. B. Verletzung der Fürsorge- und Erziehungspflichten, sexueller Missbrauch oder Misshandlungen von Kindern und Jugendlichen usw.) verurteilt worden sind. Um dies zu überprüfen, sind die Träger gehalten, sich bei der Einstellung und in regelmäßigen Abständen von diesen Personen ein Führungszeugnis nach § 30 Abs. 5 und § 30a Abs. 1 des Bundeszentralregistergesetzes vorlegen zu lassen. Es handelt sich hierbei um Regelungen zu einem erweiterten Führungszeugnis, welches über Personen erteilt werden kann, die beruflich, ehrenamtlich oder in sonstiger Weise kinder-

oder jugendnah tätig sind oder tätig werden sollen. Der TLfDI bat um eine Änderung der in § 5 Abs. 10 des Entwurfs zur Änderung des ThürSchfTG gewählten Formulierung, da diese nahelegte, dass der private Träger der Schule das erweiterte Führungszeugnis nach der Vorlage durch die Lehrkraft bei sich speichert. Dies war nach Auffassung des TLfDI nicht zulässig und nach der Gesetzesbegründung auch offensichtlich nicht gewollt. Der TLfDI sah darüber hinaus keinen Grund, das erweiterte Führungszeugnis beim Träger auf Dauer aufzubewahren. Es reicht danach völlig aus, wenn in den Akten vermerkt ist, dass das Zeugnis vorgelegt wurde und keine Einträge vorhanden sind. Das am ersten Januar 2016 in Kraft getretene Gesetz hat die Änderungsvorschläge des TLfDI berücksichtigt.

Schulen in privater Trägerschaft müssen sich bei der Einstellung von Lehrkräften ein erweitertes Führungszeugnis vorlegen lassen und die Vorlage sowie die Tatsache, dass keine relevanten Eintragungen hierin enthalten sind, in Akten speichern. Danach ist das Führungszeugnis an die betroffene Lehrkraft zurückzugeben.

14.26 Schule erhebt Gesundheitsdaten

Die Eltern eines Schulkindes beschwerten sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die Schule eine Liste führte, in der die Namen von erkrankten Kindern und die jeweilige Krankheitsursache eingetragen wurden. Daraufhin wandte sich der TLfDI an die betreffende Schule und forderte diese zu einer Stellungnahme zu dem erhobenen Vorwurf auf. Die Schule verwies in ihrer Antwort auf § 5 Abs. 1 der Thüringer Schulordnung, wonach die Schule über den Grund des Fernbleibens vom Unterricht unverzüglich zu informieren ist. Die Schule legte die Liste bei, in der die Sekretärin entsprechende Krankmeldungen der Eltern fortlaufend mit Datum, Klasse, Name, Vorname sowie Bemerkungen eingetragen hatte. Der TLfDI stimmte insoweit mit der Auffassung der Schule überein, als die Eltern die Schule unverzüglich über den Grund des Fernbleibens ihres Kindes zu unterrichten haben. Hierfür reicht es aber im Regelfall, wenn die Schule lediglich die Information erhält, dass das Kind erkrankt ist. Krankheitsnamen oder Symptome darf die Schule nicht verarbeiten (z. B. speichern) oder nutzen. Ausnahmen sind nur dann denkbar, wenn ein Kind häufig aus Krankheitsgründen im Unterricht fehlt

oder regelmäßig nicht am Sportunterricht teilnimmt. Hier darf die Schule bei den Eltern eine Begründung für die Nichtteilnahme verlangen, um zu entscheiden, ob das von der Schule akzeptiert oder aber die Vorlage eines ärztlichen Zeugnisses verlangt wird. Gemäß § 5 Abs. 2 Thüringer Schulordnung darf die Schule bei einer Erkrankung des Kindes von mehr als zehn Tagen die Vorlage eines ärztlichen Zeugnisses verlangen. Häufen sich die krankheitsbedingten Schulversäumnisse oder bestehen an der Erkrankung Zweifel, kann die Schule die Vorlage eines ärztlichen oder schulärztlichen Zeugnisses verlangen. Darüber hinaus besteht nach §§ 33, 34 Infektionsschutzgesetz (IfSG), z. B. bei Kopflausbefall, für Eltern die Pflicht, die Schule über die Krankheit zu unterrichten (§ 34 Abs. 5 IfSG). Gemäß § 16 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Vermerke über Krankheitsfehltage eines Kindes, vorliegend also die Krankheitsliste, sind daher dann zu löschen, wenn im Zeugnis die entschuldigten und unentschuldigten Fehltage eingetragen wurden. Der TLfDI forderte die Schule auf, grundsätzlich nur die Krankmeldung des Kindes durch die Eltern zu vermerken, keinesfalls aber den Grund der Erkrankung zu speichern. Dies gilt auch dann, wenn die Eltern der Schule freiwillig die Art der Erkrankung mitteilen. Die Schule hat dem TLfDI zugesagt, dies entsprechend umzusetzen.

Schulen dürfen nur speichern, welches Kind aus welcher Klasse wann und für wie lange von den Erziehungsberechtigten krankgemeldet wurde. Eine Speicherung von Krankheitsnamen oder Symptomen in den Schulunterlagen ist im Regelfall nicht zulässig. Im Falle einer Erkrankung des Kindes an einer nach dem Infektionsschutzgesetz meldepflichtigen Krankheit haben die Erziehungsberechtigten dies der Schule mitzuteilen. Die Schulleitung hat „das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen“. Gegen eine allgemeine Information der Eltern über eine in der Einrichtung aufgetretene, meldepflichtige Erkrankung, um auf bestimmte Symptome hinzuweisen, bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

14.27 Schüler an den Pranger gestellt: nichts dazu gelernt!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr durch die Beschwerde eines Schulelternsprechers von einem Vorfall in der Schule, der sich als ungeheuerlich herausstellte und bei dem das Verhalten der Schulleitung böse Erinnerungen an eine längst überwunden geglaubte Vergangenheit weckte, in deren Mittelpunkt die Erziehung der Jugend zu staatbürgerlicher Disziplin stand. Danach mussten sich auf Anweisung der Schulleitung in einer fünften Unterrichtsstunde alle anwesenden Schüler und Lehrkräfte vor dem Speisesaal der Schule versammeln. Die Schulleitung verkündete daraufhin den Grund für die kurzfristig einberufene Versammlung und führte dabei drei Punkte auf. Im letzten Punkt wurde die Erteilung eines Schulverweises angekündigt. Nach Schilderung des Elternsprechers hatten im Vorfeld bereits viele Schüler große Angst davor gehabt, ob sie das Kind sein könnten, welches den Schulverweis erhalten wird. Tatsächlich wurde dann ein bestimmter Schüler namentlich aufgerufen, neben die Schulleitung zu treten und erhielt dort vor allen Anwesenden einen strengen Schulverweis unter Benennung des Fehlverhaltens und weiterer möglicher disziplinarischer Schritte. Der TLfDI schrieb daraufhin die Schule an und wies auf die bestehenden datenschutzrechtlichen Regelungen hin. Die Regelungen zum Datenschutzgesetz ergeben sich insbesondere aus § 57 des Thüringer Schulgesetzes (ThürSchulG), der Thüringer Schulordnung sowie für ungeregelte Sachverhalte aus dem Thüringer Datenschutzgesetz (ThürDSG). Die Erteilung eines Verweises an einen Schüler vor der gesamten Schulöffentlichkeit stellt eine Übermittlung personenbezogener Daten an Dritte dar. Eine Übermittlung ist nur unter den in § 57 Abs. 4 ThürSchulG genannten sehr engen Voraussetzungen (rechtliches Interesse eines Dritten, an die Gesundheitsämter zur Durchführung schulärztlicher Untersuchungen, Vorliegen einer rechtswirksamen Einwilligung des Betroffenen) zulässig. Auch nach Auswertung der Stellungnahme der angefragten Schule hatte sich der geschilderte Sachverhalt im Großen und Ganzen bestätigt. Der TLfDI kam zu dem Ergebnis, dass es sich bei der Verfahrensweise um einen erheblichen datenschutzrechtlichen Mangel handelte. Zum einen sollte die Maßnahme nach Schilderung des Beschwerdeführers einen nachhaltigen Eindruck sowohl bei dem betroffenen Schüler als auch bei den übrigen anwesenden Schülern hinterlassen. Zum anderen erfolgte die

öffentliche Erteilung des Verweises nicht aus einem fahrlässigen Versehen heraus, sondern durchaus in der Absicht, die dabei entstandene Prangerwirkung der Situation dafür zu nutzen, ein Exempel zu statuieren und für die anderen Schüler als abschreckendes Beispiel zu dienen. Der TLfDI sprach der Schule eine Beanstandung gemäß § 39 Abs. 1 ThürDSG aus. Wie zu erfahren war, wurde der Vorfall ebenfalls fachaufsichtlich vom zuständigen Staatlichen Schulamt geprüft und der Schulleitung eine dienstliche Rüge erteilt.

Schulen haben vor einer Übermittlung personenbezogener Schüler-, Eltern- und Lehrerdaten die rechtlichen Voraussetzungen für die Zulässigkeit der Übermittlung zu prüfen. Zumindest aus datenschutzrechtlicher Sicht ist eine Übermittlung personenbezogener Schülerdaten an die Schulöffentlichkeit zum Zwecke der Disziplinierung von Schülern grundsätzlich unzulässig. In Zweifelsfällen sollte die Schule sich an den im jeweiligen Schulamt für die Schulen zuständigen Beauftragten für den Datenschutz oder gerne auch an den TLfDI wenden.

14.28 Datenschutzrechtliches O. K. für Schulportal?

Das Medienzentrum Jena bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beurteilung einer konkreten Schulportallösung. Es ist angedacht, das Verfahren als Kommunikationsplattform zwischen den Schülerinnen, Schülern und Lehrkräften in den Schulen der Stadt Jena einzusetzen. Das Schulportal bietet dabei zahlreiche Funktionen zur Nutzung an, etwa Zugriffe auf von der Schule bereitgestellte Informationen und Unterlagen, Unterrichtsmaterialien, Vertretungspläne, Stundenpläne, Aktuelles etc. Weiterhin können Lehrkräfte sowohl von der Schule aber auch von zu Hause aus in Hausaufgaben und andere Arbeitsergebnisse von Schülern Einblick nehmen, diese kommentieren oder bewerten. Die Schülerinnen und Schüler haben die Möglichkeit, bei der Bildung einer Lern- oder Projektgruppe eigene virtuelle Räume mit Chat und Blogfunktion einzurichten. Der TLfDI hatte das Verfahren anhand der vom Medienzentrum Jena vorgelegten Unterlagen einer ersten datenschutzrechtlichen Prüfung unterzogen. Zunächst wurde dabei festgestellt, dass im Gegensatz zu den Angaben des Medienzentrums das Schulportal nicht von einem anderen Landesdatenschutzbeauftragten bereits eine Zustimmung erhalten hatte. Die

weitere Systemprüfung ergab, dass die Datenübertragung auf allen Übertragungswegen mit einer TLS / SSL Verschlüsselung – es handelt sich um ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet – abgesichert werden kann, wozu auch ein eigenes Zertifikat vorhanden ist. Aus technischer Sicht gibt es nur wenige Einwände gegen das System. Die getroffenen technischen und organisatorischen Maßnahmen entsprechen insoweit dem Stand der Technik. Offen ist hier noch, ob Nutzer bei der Rechte- und Passwortübernahme explizit ausgenommen werden können, etwa aufgrund einer fehlenden Einwilligung. Ebenfalls ist ungeklärt, wie das Löschkonzept aussieht, also ob z. B. nach Ausscheiden von Schülerinnen und Schülern eine automatische Löschung des Nutzers erfolgt oder ob dies von den Betroffenen beantragt werden muss und wer die Einhaltung von Löschfristen überwacht. Soweit die Schulen dieses Schulportal einführen wollen, müssen diese mit dem Unternehmen, welches für das Verfahren Dienstleistungen hinsichtlich der IT-Systembetreuung für die Hard- und Software erbringt und bei denen Mitarbeiter des Unternehmens mit personenbezogenen Daten der Schulen in Kontakt kommen können, etwa bei der Wartung, einen Auftragsdatenverarbeitungsvertrag gemäß § 8 Thüringer Datenschutzgesetz (ThürDSG) abschließen. Die Schulen haben auch zu prüfen, ob die schulrechtlichen Voraussetzungen für die Einführung dieses Verfahrens gegeben sind. Das Schulportal bedarf vor der Nutzung gemäß § 34 Abs. 2 ThürDSG zunächst hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung der vorherigen schriftlichen Freigabe durch die Stelle, die nach Absatz 1 den Datenschutz sicherzustellen hat. Dies sind vorliegend die staatlichen Schulämter oder das Thüringer Ministerium für Bildung, Jugend und Sport. Ebenfalls muss das Schulportal zum Verfahrensverzeichnis nach § 10 ThürDSG aufgenommen werden. Zusätzlich ist ein Sicherheitskonzept nach § 9 Abs. 2 Satz 1 ThürDSG zu erstellen und eine Dienstanweisung zur Nutzung des Systems anzufertigen. Darüber hinaus muss von den Schulen beachtet werden, dass in Verfahren die Verschlüsselung mittels HTTPS als Transportverschlüsselung sichergestellt wird. Weiterhin ist die Schule selbst für die Datensicherung der Nutzerdateien zuständig. Außerdem müssen vor der Systemeinrichtung die Nutzungsbedingungen bekannt gemacht und die Einwilligungserklärungen eingeholt werden. Der TLfDI hält eine verpflichtende Teilnahme an dem Schulportal ohne eine schulgesetzliche Ergänzung nicht für zulässig. Das Medienzentrum Jena teilte

dem TLfDI auf der Grundlage seiner datenschutzrechtlichen Prüfung mit, das Projekt weiterzuverfolgen und den TLfDI hierüber zu unterrichten.

Auch wenn ein Schulportal aus datenschutzrechtlicher Sicht grundsätzlich die Ausführung der Bestimmungen des ThürDSG gewährleistet, hat die Schule bei der konkreten Nutzung eines solchen Systems zahlreiche technische und organisatorische Maßnahmen zu treffen, um einen datenschutzgerechten Verfahrensablauf zu gewährleisten.

14.29 Datenunfall bei Schülern? – Prüfung einer Panelstudie

Im Vorfeld einer an mehreren Thüringer Schulen geplanten Panelstudie, also einer Langzeit- und Längsschnittstudie, die über einen Zeitraum von sechs Jahren (5. bis 10. Klassenstufe) angelegt ist, wandte sich ein Forschungsinstitut an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um datenschutzrechtliche Prüfung des Forschungsvorhabens. Die Zielsetzung der Studie war es, zu untersuchen, aus welchen Gründen es bei Schülerinnen und Schüler zu Unfällen sowie Verletzungen im schulischen Bereich kommt und welche Möglichkeiten der Vorbeugung ergriffen werden können. Die Forscher gingen dabei von der These aus, dass Unfälle sich nicht allein zufällig ereignen, sondern dass auch das familiäre und soziale Umfeld der Jugendlichen einen Einfluss ausübe. Die Datenerhebung erfolgte auf freiwilliger Basis, wobei Schüler und Eltern gebeten wurden, ihre schriftliche Einwilligung zur Teilnahme an der Studie zu erklären. Die Datenerhebung am Befragungstag wurde computergestützt mit Tablet-PCs im Offline-Modus durchgeführt, wobei jedem teilnehmenden Jugendlichen ein Gerät ausgehändigt wurde, auf dem der dort aufgespielte Fragebogen direkt bearbeitet werden sollte. Die Antworten wurden lokal auf den Tablets abgespeichert. Die Jugendlichen mussten bei der Beantwortung der Fragen ihre Namen nicht nennen, jedoch einen individuellen Code generieren. Das Forschungsinstitut bezeichnete die Befragung als faktisch anonym. Aufgrund der Vielzahl der Angaben konnte aber mit Zusatzwissen eine Personenbeziehbarkeit nicht vollständig ausgeschlossen werden.
Auf Anfrage des TLfDI, ob und auf welche Weise sichergestellt sei, dass eine Einsicht in die Antworten des befragten Jugendlichen nach

Rückgabe des Tablets durch Dritte verhindert wird, teilte das Forschungsinstitut mit, dass das Anwendungsprogramm keine Möglichkeit zulässt, mit herkömmlichen Anwendungen Zugriff auf die gespeicherten Antworten zu erhalten. Ebenfalls fragte der TLfDI nach, welche Zugriffsrechte auf die Rechner des Instituts bestanden, nachdem die Befragungsergebnisse von den Tablets dorthin zur weiteren Auswertung hochgeladen worden waren. Nach Angaben des Instituts war der Zugriff auf die gespeicherten Daten nur durch die Benutzung persönlicher passwortgeschützter Anmeldezugänge möglich, wobei sich die Rechner in abschließbaren Büros befanden. Der TLfDI informierte das für die Genehmigung zur Durchführung der Studie an den staatlichen Thüringer Schulen zuständige Thüringer Ministerium für Bildung, Jugend und Sport über sein Schreiben an das Institut und erhielt vom Ministerium die Antwort, dass die Befragung genehmigt worden sei. Inzwischen hat das Forschungsinstitut dem TLfDI Unterlagen über die zweite Erhebungswelle der Panelstudie mit der Bitte um erneute Prüfung vorgelegt. Wie sich zeigte, wurden lediglich einige Änderungen im Schülerfragebogen vorgenommen, während die organisatorische und technische Durchführung der Untersuchung praktisch gleich blieb. Der TLfDI hat deshalb gegen die Fortführung der Studie keine Bedenken geäußert.

Auch wenn bei Schulstudien an den staatlichen Schulen des Freistaats Thüringen eine Einwilligung der Erziehungsberechtigten und der Schülerinnen und Schüler vorliegt, dürfen die Studien nur durchgeführt werden, wenn von der verantwortlichen Forschungsstelle die nach § 9 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten.

14.30 Schule – Videogaga 8

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Anfrage einer Berufsfachschule zu einer geplanten Videoüberwachung im Erdgeschoss ihres Schulgebäudes. Die geplante Videoüberwachung sollte nur außerhalb der Unterrichtszeiten der Berufsfachschule erfolgen. Während des Schulbetriebes sollten das System deaktiviert und die Videokameras für jedermann ersichtlich

auf die Wand ausgerichtet werden. Die Speicherung der erhobenen Daten sollte nicht länger als maximal sieben Tage betragen.
Zunächst stellte der TLfDI fest, dass die Berufsfachschule als Schule in freier Trägerschaft den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes (BDSG) unterliegt. Rechtsgrundlage für den Einsatz von Videoüberwachung in öffentlich zugänglichen Bereichen ist § 6b BDSG, für nicht öffentlich zugängliche Bereiche gilt § 28 BDSG. Außerhalb der Schulzeit ist das Schulgebäude nicht öffentlich zugänglich. Die Videoüberwachung in nicht öffentlich zugänglichen Räumen außerhalb der Schulzeit richtet sich nach § 28 Abs. 1 Nr. 2 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Da außerhalb der Schulzeit die Schule nicht dazu bestimmt ist, von einem unbestimmten Personenkreis betreten und genutzt zu werden, bestand nach Auffassung des TLfDI kein Grund zur Annahme, dass schutzwürdige Interessen von Betroffenen berührt sind. Die Videoüberwachung war daher zu diesen Zeiten grundsätzlich als zulässig anzusehen.
Etwas anderes ergibt sich dann, wenn außerhalb der Schulzeiten Räume oder Flächen der Schule für die Öffentlichkeit freigegeben werden. Hierzu zählen etwa die Aula bei öffentlichen Konzerten oder Feierstunden, eine Sporthalle, die von Vereinen genutzt wird, die Vermietung von Klassenräumen für außerschulische Kurse usw. Auch sollte dabei an eine Reinigungsfirma gedacht werden, die die Schulräume außerhalb der Unterrichtszeiten reinigt und somit bei der Erledigung der Arbeit beobachtet und aufgezeichnet werden würde. Ebenso liegt eine Videoüberwachung von öffentlich zugänglichen Räumen vor, wenn die Beobachtung sich auf weitere Bereiche über die Schule hinaus erstreckt, in denen sich Personen zulässigerweise aufhalten dürfen, z. B. auf öffentlichen Verkehrswegen rund um das Schulgebäude oder innerhalb und außerhalb des Schulgebäudes, wenn diese Bereiche nach dem erkennbaren Willen des Grundstückeigentümers oder des Trägers von jedermann genutzt oder betreten werden dürfen. In den vorgenannten Fällen liegt eine Beobachtung öffentlich zugänglicher Räume vor, die gemäß § 6b Abs. 1 Nr. 2 und 3 BDSG nur zulässig ist, soweit sie zur Wahrnehmung des Haus-

rechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da in den genannten Beispielen schutzwürdige Interessen von Betroffenen bestehen, darf hier die Videoüberwachung nur erfolgen, wenn z. B. Vorkommnisse nachgewiesen werden (Einbrüche, Vandalismus), aus denen sich eine Erforderlichkeit der Videoüberwachung ergibt.
§ 6b Abs. 2 BDSG verlangt außerdem, dass auf jede Form der Videoüberwachung und auf die verantwortliche Stelle hingewiesen wird. Ausdrücklich vorgesehen ist dies zwar nur für die Videoüberwachung öffentlich zugänglicher Räume. Es empfiehlt sich jedoch auch bei einer Videoüberwachung nicht öffentlich zugänglicher Räume, aus Gründen der Transparenz entsprechende Hinweisschilder oder Piktogramme anzubringen, vgl. § 4 Abs. 3 BDSG.
Die von der Berufsfachschule geplante Löschfrist von sieben Tagen war nach Auffassung des TLfDI zu lang. Eine Löschung der Aufnahmen sollte regelmäßig nach 48 Stunden erfolgen, es sei denn, es liegen besondere Gründe für eine längere Speicherung vor (Feiertage, Wochenende).
Diese Rechtsauffassung wurde der Berufsfachschule mitgeteilt, die sich daraufhin nicht mehr gemeldet hat.

Eine Videoüberwachung an und in Schulen kann nur ausnahmsweise und grundsätzlich nur außerhalb der Unterrichtszeiten gerechtfertigt sein. Auch dann müssen allerdings die schutzwürdigen Interessen von Personen, die sich zu dieser Zeit zulässigerweise auf dem Schulgelände oder in den Schulgebäuden aufhalten, hinreichend berücksichtigt werden.

14.31 Sicheres soziales Netzwerk für Thüringer Schulen!

In unserer digitalen Welt richten Datensammler wie Datenschützer ihre Augen auf die neuen Kommunikationswege. Sichere Briefpost ist fast out. Ohne E-Mail und Kurznachrichten, ohne Chat und Cloud geht heute praktisch nichts mehr. Auch Lehrer mailen natürlich mit ihren Schülern und deren Eltern, zu ihren Kollegen und Schulleitern, das Bildungsministerium mailt zu Schulämtern, Schulämter zu Schulen, zu Schulverwaltungen usw., usw. Geht es da immer datenschutzgerecht zu? Auf jeden Fall bestehen datenschutzrechtliche

Hürden, wenn die Inhalte solcher Nachrichten personenbezogene Daten enthalten. Und das dürfte bei einem Großteil schulbezogener Mitteilungen der Fall sein. Dass soziale Netzwerke wie Facebook für die Nachrichtenübermittlung in schulischem Kontext keine Rolle spielen dürfen, hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits Mitte 2013 in einer Pressemitteilung öffentlich klargestellt und alle Thüringer Schulen besonders informiert. Das heißt natürlich nicht, dass soziale Netzwerke im Unterricht keine Rolle spielen dürfen. Im Gegenteil: Neue Kommunikationsformen mit ihren Möglichkeiten und Gefahren müssen Thema in zeitgemäßem Unterricht sein.
Aber auch E-Mails sind bekanntermaßen wie Postkarten, die jeder lesen kann, wenn er das notwendige Know-how besitzt, um sie aus dem Netz zu fischen. Abhilfe schafft hier die Ende-zu-Ende-Verschlüsselung, die aber den meisten Lehrern noch immer unbekannt ist oder zu kompliziert erscheint. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bietet deshalb Schulungen zur E-Mailverschlüsselung für Lehrer an (siehe dazu Anlage 86). Ein anderer Ansatz des TLfDI besteht darin, für alle o. g. Personengruppen eine einheitliche, handhabbare Kommunikationsplattform zu empfehlen – einen geschützten Raum, der den gezielten Informationsaustausch ermöglicht, aber die Nachrichten vor fremden Blicken sicher schützt. Dieses Rad muss nicht neu erfunden werden, denn moderne Lernplattformen, die teilweise auch an Thüringer Schulen als „virtuelle Klassen- oder Lehrerzimmer“ genutzt werden, besitzen die notwendigen Funktionen für einen gezielten Nachrichtenaustausch zwischen Einzelpersonen und Personengruppen bereits. Selbstverständlich sind dabei eine verlässliche Nutzerregistrierung und angemessene Rechtevergabe erforderlich, damit die elektronische Post, z. B. mit einer Zeugnisbeurteilung oder einem Sonderpädagogischen Gutachten, keine Abwege gehen kann. Der TLfDI prüft seit Anfang 2015 solche Plattformen mit dem Ziel, dem zuständigen Bildungsministerium konkrete Vorschläge zu unterbreiten, die schul- und datenschutzrechtskonform sind. Ziel ist es, eine datenschutzgerechte Lösung für Thüringer Schulbehörden und alle Schulen in Thüringen zu schaffen, die öffentliche Stellen im Sinne des Thüringer Datenschutzgesetzes sind.
Auf Bundesebene beschäftigt sich derzeit auch der Arbeitskreis Datenschutz und Bildung der Datenschutzbehörden des Bundes und der Länder, dessen Vorsitzender der TLfDI ist, mit dieser Frage.

Nachrichten werden heute in der Regel elektronisch ausgetauscht. Das gilt auch für den dienstlichen Austausch zwischen Lehrern, Schülern, Eltern, Schulbehörden usw. Hier bestehen datenschutzrechtliche Hürden, weil dabei regelmäßig personenbezogene Daten verarbeitet (erhoben, übermittelt, gespeichert) werden. Facebook und andere soziale Netzwerke sind hier tabu. Der TLfDI prüft seit 2015, ob eine geschützte Lernplattform für alle Thüringer Schulen und Schulbehörden eine datenschutzgerechte Alternative sein kann.

14.32 Schweigepflichtentbindung an einer Schule

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage einer Staatlichen Regelschule aus Thüringen. Sie bat um Überprüfung des Formulars zur Einwilligungserklärung zur Übermittlung personenbezogener Daten der Schüler von den Erziehungsberechtigten an andere Stellen, wie Ärzte, Schulpsychologen, Sozialarbeiter und Ehe-, Familien- und Schwangerschaftsberater. Dabei ging es nicht um die Frage, wer die Einwilligung im Einzelfall zu erteilen hat, die Eltern oder (auch) die Schüler, sondern um den notwendigen Inhalt der Einwilligungserklärung.
Da das Thüringer Schulgesetz keine spezielle Regelung zur Einwilligung des Betroffenen in die Verarbeitung seiner Daten enthält, findet das Thüringer Datenschutzgesetz (ThürDSG) Anwendung. Nach § 4 Abs. 2 ThürDSG ist die Einwilligung eine auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung und der Nutzung zuzustimmen. Wird die Einwilligung beim Betroffenen eingeholt, ist er auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folge der Verweigerung der Einwilligung hinzuweisen, § 4 Abs. 3 ThürDSG. Die Verarbeitung oder das Nutzen von Daten über die Gesundheit ist nur zulässig, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht, § 4 Abs. 5 Nr. 2 ThürDSG.
Aus der Sicht des TLfDI erfüllte die von der Staatlichen Regelschule vorgelegte Form der Einwilligung nicht die gesetzlichen Voraussetzungen. Es handelte sich um eine pauschale Einwilligung, in der

bestimmte Stellen angekreuzt werden konnten. Der Zweck der Datenverarbeitung war sehr allgemein damit bezeichnet, die schulischen Leistungen des Kindes zu fördern und eine soziale Eingliederung zu unterstützen. Sofern ein Arzt von seiner Schweigepflicht entbunden und die datenschutzrechtliche Einwilligung zur Datenverarbeitung gegeben werden sollte, müssten der Arzt sowie der Schulpsychologe oder der Sozialarbeiter konkret namentlich benannt werden. In dem Formular war für den TLfDI nicht eindeutig dargelegt, ob in die Datenerhebung bei dem Arzt, Schulpsychologen und bei den sonstigen genannten Stellen eingewilligt werden sollte oder ob in die Datenübermittlung an diese Stellen eingewilligt wurde. Außerdem gab es entgegen der gesetzlichen Regelung in dem zur Überprüfung vorgelegten Formular keine Angaben zur Dauer der Speicherung sowie keinen Hinweis auf die Rechte der Auskunftserteilung, Berichtigung oder Löschung.
Im Ergebnis empfahl der TLfDI der Staatlichen Regelschule, in den Fällen, in denen eine Datenerhebung bei Dritten zukünftig erforderlich ist, diese Stelle konkret zu benennen und den konkreten Zweck der Erhebung zu bezeichnen. Die möglicherweise zu erhebenden Daten könnten dann, wie es in dem Formblatt bereits angelegt war, jeweils angekreuzt werden. Diese Stellungnahme teilte der TLfDI der Staatlichen Regelschule mit.

Nach § 4 Abs. 2 ThürDSG ist die Einwilligung eine auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung und der Nutzung zuzustimmen. Wird die Einwilligung beim Betroffenen eingeholt, ist er auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folge der Verweigerung der Einwilligung hinzuweisen, § 4 Abs. 3 ThürDSG.

14.33 Schulunterricht online

Der unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) tagende Unterarbeitskreis Datenschutz und Schule der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat im vorliegenden Berichtszeitraum sehr intensiv an einer gemeinsame Orientierungs-

hilfe für Online-Lernplattformen gearbeitet. Damit wollten die Datenschutzbeauftragten auf die Entwicklung reagieren, dass immer mehr Bildungsinstitutionen und hierunter insbesondere die Schulen auf die internetgestützte Vermittlung von Wissen und den elektronischen Kontakt zwischen Schülern und Lehrern setzen. Für Online-Lernplattformen hat sich inzwischen ein großer Markt gebildet, auf dem Schulbuchverlage sowie Computer- und Softwarehersteller zahlreiche Produkte anbieten. Eine Online-Lernplattform ist ein Softwaresystem, das den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation des Schulstoffes ergänzt oder sogar ersetzt. Der Zugriff auf die Software erfolgt ortsunabhängig mit einem Endgerät (PC, Tablet, Smartphone) über einen Web-Browser (Computerprogramm zur Darstellung von Webseiten im Internet). Die computerbasierte Lernumgebung kann von der Schule auf unterschiedliche Weise gestaltet werden, etwa durch das Einrichten von Kommunikationswegen zwischen Lehrer und Schüler, der Durchführung von Gruppenarbeit, der Erteilung von Aufgaben zur Übung oder zur Lernkontrolle. Grundsätzlich besteht für die Schule die Möglichkeit, eine Online-Lernplattform in Form einer freiwilligen Beteiligung der Schüler oder aber als verpflichtende Teilnahme zu organisieren. In letzterem Fall hat die Schule die faktische Teilnahme der Schüler zu gewährleisten. Aus datenschutzrechtlicher Sicht werden mit dem Verfahren auch viele personenbezogene Schüler- und Lehrerdaten internetbasiert verarbeitet. Aus diesem Grund soll die Orientierungshilfe als Hilfestellung für die Schulverwaltung und die Schulen dienen, welche datenschutzrechtliche Mindestkriterien Online-Lernplattformen erfüllen müssen. Zusätzlich werden den Anbietern von Online-Lernplattformen Kriterien an die Hand geben, wie ihr jeweiliges Produkt gestaltet oder angepasst werden muss, damit eine Nutzung durch die Schulen auf zulässige Weise erfolgen kann. Jeder Schüler muss sich als Zugangsvoraussetzung zunächst im Onlineverfahren auf der Lernplattform anmelden. In aller Regel melden sich die Benutzer einer Plattform personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. Hierdurch entsteht die Gefahr, dass Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt und Informationen ermittelt werden. Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung der Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen den Lehr-

kräften erheblich mehr Daten zur Verfügung, als für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen. Beim Einsatz von Online-Lernplattformen wird Lehrkräften die Möglichkeit eingeräumt, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wann, wie oft und zu welchen Zeiten ein Schüler in der Online-Lernplattform an bestimmten Aufgaben gearbeitet hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Bei der Nutzung von Lernplattformen bleibt die Schule – oder je nach Bundesland die Schulaufsichtsbehörde – verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus, dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten“ bleibt. Bei der Auswahl bzw. Anschaffung einer Online-Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser Anbieter die schuldatenschutzrechtlichen Anforderungen erfüllen kann oder ob die Schule / die Schulaufsichtsbehörde gegebenenfalls ein eigenes Lernportal erstellt. Weiterhin ist das Verfahren nach § 34 Abs. 2 ThürDSG zuvor von der Schulaufsichtsbehörde schriftlich freizugeben und nach § 10 ThürDSG in das Verfahrensverzeichnis aufzunehmen. Schüler, Eltern und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich zu unterrichten. Sie sind darüber aufzuklären, dass sie nach § 10 Abs. 3 Thüringer Datenschutzgesetz berechtigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht hinzuweisen. Außerdem sind die Lehrkräfte und Administratoren zu schulen und die Schüler zu unterweisen.

Eine endgültige Fassung der Orientierungshilfe konnte erst nach dem Berichtszeitraum fertiggestellt werden. Sie ist unter https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh-lernplattformen.pdf veröffentlicht.

Der Einsatz von Online-Lernplattformen in der Schule liegt im Trend. Da mit diesen Verfahren zahlreiche personenbezogene Schü-

ler- und Lehrerdaten verarbeitet und genutzt werden, sind alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Eine Orientierungshilfe „Online-Lernplattformen“ gibt sowohl den Anbietern als auch den Nutzern dieser Systeme wertvolle Hinweise, welche datenschutzrechtlichen Mindestkriterien beim Einsatz zu beachten sind.

14.34 Daten-Wolken auch für Schulen?

Datenwolken wabern überall und sind bereit, ganze Festplatteninhalte in sich aufzusaugen, wenn das der Kunde will. Es ist ja auch ganz vorteilhaft, von jedem Ort der Welt auf seine Daten zugreifen zu können. Das könnte auch für Schulen und Schüler interessant sein, wenn es darum geht, z. B. Unterrichtsvideos und andere datenintensive Inhalte für sich und seine Schüler verfügbar zu haben. Auch für die Schulverwaltung könnten aktuelle, gemeinsam nutzbare Datenbestände hilfreich sein. Aber wie sieht’s da mit dem Datenschutz aus? Gibt es Regelungen, ob und wie kommerzielle Cloud-Angebote, wie „Microsoft Office 365“ oder „Google Docs“ durch staatliche Schulen genutzt werden können oder nicht? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde durch eine Anfrage einer deutschen Universität mit der Frage konfrontiert, ob und wie Cloud-Lösungen an Thüringer Schulen eingesetzt werden. Dem TLfDI war hierzu nichts bekannt. Das für Schulen zuständige Ministerium teilte auf Nachfrage mit, dass es hierzu derzeit keine Richtlinie oder Empfehlungen für Schulen gäbe, weil ein Cloud-Einsatz an Schulen bislang kaum erfolge. Das könne sich aber schnell ändern. Das Bildungsressort regte deshalb an, gemeinsam mit dem TLfDI eine Empfehlung für die datenschutzgerechte Cloud-Nutzung zu erarbeiten, um zu verhindern, dass personenbezogene Daten von Thüringer Schülern, Lehrern und Eltern aus trüben Wolken ausländischer Server irgendwo abregnen. Nach § 9 Thüringer Datenschutzgesetz (ThürDSG) hat die Daten verarbeitende Stelle die technischen und organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um die bestehenden datenschutzrechtlichen Regelungen einzuhalten. Bei Cloud-Angeboten aus dem außereuropäischen Ausland besteht immer die Frage, ob dort ein angemessenes Datenschutzniveau im Sinne von § 23 Abs. 1 Satz 2 ThürDSG besteht. Nach dem Aus für Safe-Harbor bestehen hier bei

Angeboten aus den Vereinigten Staaten erhebliche Zweifel (siehe dazu Nr. 3.1). Es gilt zu vermeiden, dass die Schule als verantwortliche Stelle Rechtsverstöße begeht. Der sinnvolle Vorschlag des Bildungsministeriums wird derzeit vom TLfDI geprüft.

Die Nutzung internetbasierter Datenspeicher gewinnt allgemein an Bedeutung. Der Trend geht vermutlich auch an Schulen und Schulbehörden nicht vorbei. Um solche Möglichkeiten datenschutzgerecht zu gestalten, bedarf es Vorkehrungen und fundierter Empfehlungen für die Nutzer. Der TLfDI prüft den Vorschlag des Bildungsressorts, gemeinsam eine Empfehlung für die Schulen zu erarbeiten.

14.35 Behördliche Datenschutzbeauftragte an Schulen

Wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in den letzten zwei Tätigkeitsberichten (9. Tätigkeitsbericht unter Punkt 13.2 und 10. Tätigkeitsbericht unter 13.2) dargestellt hatte, wurde in jedem staatlichen Schulamt jeweils eine dort beschäftigte Person als Beauftragter für den Datenschutz (bDSB) nach § 10a Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) für alle staatlichen Schulen im Zuständigkeitsbereich bestimmt.
Hinsichtlich der in den Schulen eingesetzten Hard- und Software zur Verarbeitung von Schüler-, Eltern- und Lehrerdaten bestand zwischen dem TLfDI und dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) weiterhin Uneinigkeit darüber, ob die Schule oder aber der kommunale Schulträger Daten verarbeitende Stelle im Sinne von § 3 Abs. 5 ThürDSG ist. Dies ist aber entscheidend für die Frage, welche Stelle die Verantwortung für die Sicherstellung des Datenschutzes trägt und damit die Verfahren nach § 34 Abs. 2 ThürDSG vor dem erstmaligen Einsatz freizugeben hat. Der Zweck der datenschutzrechtlichen Freigabe liegt in der Vorabkontrolle der Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten. Automatisierte Verfahren dürfen grundsätzlich erst nach der vorherigen schriftlichen Freigabe eingesetzt werden. Weiterhin hat die Daten verarbeitende Stelle gemäß § 10 ThürDSG ein Verzeichnis der automatisierten Verfahren zu führen, mit denen personenbezogene Daten verarbeitet werden. Dies dient der Eigenkontrolle der Behörde und als Grundlage für die Kontrollen des TLfDI. Es dient darüber hinaus der Transparenz der Datenverar-

beitung innerhalb der öffentlichen Stelle. Entsprechend § 10a ThürDSG ist dem Beauftragten für den Datenschutz die Führung des Verzeichnisses und folglich die Zuständigkeit für die Publizität der automatisierten Verfahren als Aufgabe übertragen worden. Zusätzlich hat die Daten verarbeitende Stelle nach § 9 Abs. 2 ThürDSG ein Sicherheitskonzept zu erstellen, auf dessen Grundlage die in der Schule zur Gewährleistung von Datenschutz und Datensicherheit zu treffenden technischen und organisatorischen Maßnahmen ermittelt werden müssen. Eine weitere Zuständigkeitsproblematik ergab sich aus der Wartung, der Ergänzung oder durch den Austausch der in der Schule eingesetzten automatisierten Datenverarbeitungsanlagen, die im Regelfall entweder vom Schulträger selbst oder von einer privaten Stelle vorgenommen werden. Nach der Argumentation des TMBWK finanziert der Schulträger die Infrastruktur der Schule, wozu auch die angeschaffte Hard- und Software gehört, und hat den laufenden Betrieb sicherzustellen. Aufgrund des kommunalen Selbstverwaltungsrechts steht es in eigener Verantwortung des Schulträgers, was er wann auf welche Weise beschafft und wie er den Betrieb sicherstellt, um den schulgesetzlichen Vorgaben gerecht zu werden. Aber bereits aus der gesetzlichen Definition des § 3 Abs. 5 ThürDSG wird deutlich, dass die Daten verarbeitende Stelle Daten in eigener Verantwortung für sich selbst verarbeitet oder nutzt oder dies im Auftrag durch andere vornehmen lässt. Der Schulträger verarbeitet aber keine schulischen Daten der Schüler, Eltern und Lehrer. Hierfür ist ausschließlich die Schule zur Erfüllung ihrer Aufgaben zuständig. Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt gemäß § 8 Abs. 1 ThürDSG der Auftraggeber für die Einhaltung der Bestimmungen dieses Gesetzes verantwortlich. In § 8 Abs. 7 ThürDSG ist ausdrücklich geregelt, dass die Vorschrift auch entsprechend für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen gilt, soweit ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann. Daher ist die Schule als Auftraggeber verpflichtet, mit dem Schulträger als Auftragnehmer eine vertragliche Vereinbarung über die Wartung abzuschließen. Zu den Aufgaben der bDSB gehört es, die Schulen bei der Ausführung des ThürDSG und anderer Rechtsvorschriften über den Datenschutz zu unterstützen und auf deren Einhaltung hinzuwirken. Aus diesem Grund lud der TLfDI die bDSB der staatlichen Schulämter wie ein Jahr zuvor zu einer Gesprächsrunde ein, in der besprochen wurde,

welchen Stand bis dahin die Erstellung der datenschutzrechtlichen Freigaben, Verfahrensverzeichnisse, Sicherheitskonzepte und Verträge über Auftragsdatenverarbeitungen zwischen Schule und Schulträger erreicht hatte. Weitere Themen waren die Frage nach der Verantwortung für den Betrieb einer Schulhomepage, die wahrgenommenen Weiterbildungsmaßnahmen zur Erweiterung der Fachkunde für bDSB und das von den staatlichen Schulämtern zur Verfügung gestellte Zeitkontingent für die Erledigung der Aufgaben des bDSB. Aus den Darlegungen der bDSB konnte der TLfDI entnehmen, dass die Fortschritte bei der Umsetzung der erforderlichen Freigaben und Verfahrensverzeichnisse im Vergleich der staatlichen Schulämter sich voneinander unterschieden, insgesamt aber nur eine sehr geringe Anzahl von automatisierten Schulverwaltungsverfahren bereits freigegeben und in das Verfahrensverzeichnis eingetragen waren. Hinsichtlich der Erstellung eines IT-Sicherheitskonzeptes für die Schulen, musste der TLfDI konstatieren, dass bis dahin für keine Schule ein solches Konzept vorlag. Mit der Problematik der Wartung der automatisierten Datenverarbeitungsanlagen der Schulen durch die kommunalen Schulträger in Auftragsdatenverarbeitung hatten sich die bDSB bis dahin ebenfalls nicht beschäftigt. Aufschlussreich für den TLfDI war der Hinweis einiger bDSB darauf, dass die Beschaffung der Schulsoftware nicht vom Schulträger, sondern teilweise von der Schule selbst wahrgenommen wurde. Allerdings sei es den Schulen untersagt, selbstständig Computer zu beschaffen und mit dem internen Schulcomputernetz zu verbinden. Weiterbildungsmaßnahmen im Bereich des Datenschutzes wurden lediglich von einigen bDSB bereits wahrgenommen. Die Teilnehmer wurden gebeten, mitzuteilen, ob ihnen für die Aufgabe des bDSB der Schulen ein ausreichendes Zeitbudget eingeräumt wurde. Aber auch hier gab es je nach staatlichem Schulamt unterschiedliche Regelungen. Dies war in den staatlichen Schulämtern unterschiedlich ausgestaltet. Die Spanne reichte hier von 20% der Arbeitszeit bis zu 5 % für die Aufgabe des bDSB. Aufgrund der zahlreichen übrigen Arbeitsaufgaben konnten die vom jeweiligen Schulamt eingeräumten Zeitanteile zur Wahrnehmung der Aufgabe des bDSB nicht verwendet werden. Die bDSB waren sich darin einig, dass man als bDSB zunächst mindestens 50 % der gesamten Arbeitszeit benötige. Die Festlegungen der Aufgabe eines bDSB und des eingeräumten Zeitbudgets ergaben sich nach Kenntnis der bDSB zu diesem Zeitpunkt weder aus den Geschäftsordnungen noch aus den Geschäftsverteilungsplänen der

staatlichen Schulämter. Der TLfDI nahm dies zum Anlass, die Geschäftsordnungen und -verteilungspläne bei den staatlichen Schulämtern anzufordern. Den bDSB wurde mitgeteilt, dass diese sich bei Problemen, etwa aufgrund eines nicht ausreichenden Zeitbudgets oder bei mangelnder Unterstützung durch die Behördenleitung, selbstverständlich an den TLfDI wenden können. Um sich ein Bild davon zu machen, welche Schulsoftware von den Schulen in Thüringen verwendet wird, hatte der TLfDI alle kommunalen Schulträger angeschrieben und um Mitteilung gebeten, welche Schulverwaltungssoftware dort jeweils eingesetzt wird. In Auswertung der Rückmeldungen der Schulträger war festzustellen, dass überwiegend an den Thüringer Schulen zwei unterschiedliche Schulverwaltungsprogramme eingesetzt werden, mit denen personenbezogene Schüler- und Elterndaten verarbeitet werden. Darüber hinaus wird vereinzelt weitere Schulverwaltungssoftware verwendet. Zusätzlich gibt es Teilanwendungen der Schulverwaltung, z. B. Unterrichtsplanung, Abiturverwaltung, Bibliotheksverwaltung, Notenbuch, Klassenbuch usw. Trotzdem gestaltet sich die vollständige Übersicht über die verwendeten Schulverwaltungsprogramme schwierig, da trotz grundsätzlich gleicher Programme diese mit unterschiedlichen Modulen ausgestattet sind, etwa Stundenplan, Zensur, Statistik, Haushalt, Archiv, Vertretungsplan, Datenex- und -import usw. Darüber hinaus enthalten die Programme schulartspezifische Datenbestände, je nachdem, ob das Verfahren in einer Grundschule, Regelschule, in einem Gymnasium, einer Fachschule oder Berufsschule zur Anwendung kommt. Besonderes Interesse des TLfDI weckte die Mitteilung eines Schulträgers, wonach dort nicht bekannt sei, welche Schulverwaltungssoftware eingesetzt werde, da die Schulen die Programme in eigener Verantwortung anschafften. Auch die Wartung der Programme erfolge nicht über den Schulträger. Der TLfDI gab den bDSB in den staatlichen Schulämtern dieses Ergebnis seiner Abfrage bekannt. Für eine lückenlose Erstellung der Freigaben und der Aufnahme in das Verfahrensverzeichnis müssen sich die zuständigen bDSB deshalb teilweise direkt an die Schulen in ihrem Zuständigkeitsbereich wenden. Dies insbesondere deshalb, weil die Schulen entweder das Schulverwaltungsprogramm oder zumindest Zusatzmodule hierzu selbst angeschafft haben und auch nicht bekannt ist, wer die Wartungsarbeiten der Hard- und Software durchführt. Der TLfDI wird die bDSB erneut zu einer Gesprächsrunde einladen und den bis dahin vorliegenden Stand über die erfolgten Freigaben, die

Aufnahme von Schulverwaltungssoftware in das Verfahrensverzeichnis, die Erstellung von IT-Sicherheitskonzepten sowie die Vereinbarungen über Auftragsdatenverarbeitung erfragen und für den kommenden Tätigkeitsberichtszeitraum auf die Erledigung der noch offenen Forderungen hinwirken.

Schulen dürfen Schulverwaltungsverfahren, mit denen personenbezogene Daten verarbeitet werden, nur einsetzen, wenn bestimmte formale Voraussetzungen hierfür erfüllt sind. Dies sind insbesondere die vorherige schriftliche Freigabe, das Führen eines Verfahrensverzeichnisses, das Erstellen eines IT-Sicherheitskonzeptes sowie der Abschluss von vertraglichen Vereinbarungen im Rahmen einer Auftragsverarbeitung. Den bDSB der Schulen ist für die Erledigung ihrer Aufgaben vom Dienstherrn ein ausreichendes Arbeitszeitbudget zur Verfügung zu stellen und die Möglichkeit einzuräumen, sich die notwendige Fachkenntnis anzueignen bzw. diese zu erweitern.

14.36 Veröffentlichung personenbezogener Daten des Promovenden

Ein Bürger fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob personenbezogene Daten des Verfassers einer Promotion im Internet veröffentlicht werden dürfen, obwohl der Betroffene dieser Veröffentlichung widersprochen hat. Da die näheren Umstände der Anfrage dem TLfDI nicht bekannt waren, konnte nur eine allgemeine Auskunft erteilt werden. Grundsätzlich ergibt sich aus den Promotionsordnungen der Thüringer Hochschulen, dass Dissertationen zu veröffentlichen sind. Dies betrifft neben dem Text der Dissertation auch den Namen des Promovierenden bzw. des Promovierten, das Datum der Promotion sowie den Namen der Hochschule, an der die Dissertation erfolgte. Im Regelfall wird die Veröffentlichung von Dissertationen in der Weise geregelt, dass der Promovend eine bestimmte Anzahl von Druckexemplaren im jeweiligen Fachbereich abzugeben hat bzw. die Verbreitung der Arbeit über den Buchhandel nachweisen muss. Weiterhin wird der Doktorand teilweise verpflichtet, das Recht auf Veröffentlichung seiner Dissertation in elektronischer Form in Datennetzen der Hochschule und der Deutschen Bibliothek in Frankfurt am Main und Leipzig einzuräumen. Einige Promotionsordnungen fordern zusätzlich die Abgabe von Pflichtexemplaren an die Hoch-

schule, denen der Promovend einen Lebenslauf beizufügen hat. Aus datenschutzrechtlicher Sicht muss dieser Lebenslauf lediglich über den Bildungsweg Auskunft geben. Gemäß den Promotionsordnungen sind auch die mündlichen Prüfungen öffentlich. Da eine Dissertation grundsätzlich öffentlich zugänglich ist, dürfen aus datenschutzrechtlicher Sicht die Hochschulen Namen und Vornamen sowie das Dissertationsthema im Internet veröffentlichen und das Werk zum Beispiel in der Hochschulbibliothek als Buch oder in elektronischer Form zur Verfügung stellen. Mehr noch, die Dissertation soll einen Beitrag zur Wissenschaft in einem bestimmten Gebiet leisten und der wissenschaftlichen Forschung zur Verfügung stehen. Voraussetzung hierfür ist der freie Zugang zu Dissertationen. Einer weltweiten Verfügbarkeit, also auch in Ländern, in denen kein angemessenes Datenschutzniveau gewährleistet ist, steht nichts entgegen, denn die Veröffentlichung stellt eine Datenübermittlung dar, die nach § 23 Abs. 2 Nr. 4 Thüringer Datenschutzgesetz im öffentlichen Interesse erforderlich ist. Von einem überwiegenden schutzwürdigen Interesse des Betroffenen, dessen personenbezogene Daten, soweit diese die Dissertation betreffen, nicht zu veröffentlichen, ist regelmäßig nicht auszugehen.

Ein Promovend muss davon ausgehen, dass seine Dissertation veröffentlicht wird und somit als allgemein zugängliche Quelle für wissenschaftliche Zwecke genutzt werden darf.

14.37 Sicherheitslücken bei „thoska“

Seit inzwischen 15 Jahren ersetzt die Chipkarte „thoska“ (Thüringer Hochschul- und Studentenwerkskarte) den herkömmlichen Studentenausweis in Papierform. Die Karte vereint mehrere Funktionsweisen, z. B. die Ausweisfunktion zur Sichtprüfung, sie dient als Zugriffs- und Zugangsberechtigungsnachweis, um an speziell eingerichteten Terminals zum Beispiel Ergebnisse von Prüfungsleistungen abrufen zu können. Die Karte hat auch eine Bestell- und Ausleihfunktion für Druckerzeugnisse in der Hochschulbibliothek, über sie kann der Zutritt zu Räumen oder die Durchfahrt zu Parkflächen gewährt werden. Zudem besitzt sie eine Geldbörsenfunktion bei Kopierern, in der Mensa oder beim Bezahlen von Semestergebühren. Außerdem dient sie Bediensteten der Hochschule als Zeiterfassungssystem. Presseberichten war zu entnehmen, dass die bisher teilweise

noch verwendete ältere Version der Hochschulchipkarte (Mifare Classic) von Hackern geknackt worden sei, sodass ein Missbrauch dieser Karte nicht auszuschließen ist. Die Karte konnte ausgelesen und anschließend geklont werden. Mit diesen Kopien könnten z. B. auf dem Kartenchip Geldbeträge erzeugt werden, mit denen dann in den Mensen der Studentenwerke oder an Kopierern bezahlt werden könnte. Aus datenschutzrechtlicher Sicht bedeutsam ist insbesondere die Möglichkeit der Überwindung von Türöffnungssystemen, der Identitätserschleichung beim Ausleihen von Büchern aus den Hochschulbibliotheken und der mögliche Zugriff auf Prüfungsergebnisse sowie auf weitere personenbezogene Daten, die auf der Karte gespeichert sind. Weiterhin kann die Chipkarte, da diese mit RFID-Technologie kontaktlos in einer Distanz von bis zu zehn Zentimetern arbeitet, durch ein Portemonnaie oder eine Tasche hindurch ausgelesen werden. Auf diese Weise ist es möglich, die Identität einer Person festzustellen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) schrieb daher die Hochschulen des Landes an und forderte diese auf, alle „thoska“-Chipkarten, die mit der veralteten Technik arbeiten, sofort auszusondern und durch neue Karten mit einer sicheren Technik zu ersetzen sowie die alten Karten zur Vermeidung von Missbrauch einzuziehen. Die Hochschulen haben sich nun für eine Karte entschieden, die mit einem weiterentwickelten Chip ausgestattet ist (Mifare DESFire), der mit aktuellen Kryptoalgorithmen wie zum Beispiel 2KTDES, 3KTDES oder AES128 arbeitet. Die 3DES beziehungsweise „Triple-DES“-Verschlüsselung ist dabei wesentlich sicherer, als die ursprünglich verwendete Authentifizierung über Schlüsselabgleich. Die neuen Karten sind sowohl hinsichtlich der Funktionalität als auch der Vertrauenswürdigkeit des technischen Systems nach einem internationalen Standard zertifiziert worden (Common Criteria EAL 4+). Aufgrund der Rückmeldungen der Hochschulen an den TLfDI kann die Aussage getroffen werden, dass bis Ende 2015 alle Hochschulen, die mit „thoska“ arbeiten, die alten Karten eingezogen und durch neue ersetzt haben. Dies gilt sowohl für die Studenten- als auch die Mitarbeiterkarten.

Beim Einsatz von auf RFID-Technologie basierenden Chipkarten der Thüringer Hochschulen ist der jeweilige Stand der Technik zu be-

achten, um den Schutz von personenbezogenen Daten der Hochschulangehörigen zu gewährleisten.

14.38 Prüfungsamt mit medizinischen Fähigkeiten?

In einer Kleinen Anfrage wandte sich ein Abgeordneter an die Landesregierung, weil Studierende dazu verpflichtet sind, gegenüber den Prüfungsausschüssen der Hochschulen zur Feststellung der Prüfungsunfähigkeit ihre krankheitsbedingten Beschwerden offenzulegen. Der Abgeordnete wandte sich zu dieser Problematik auch an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Darüber hinaus beschwerten sich einige Studierende über diese Verfahrensweise in ihrer Hochschule beim TLfDI. Aus datenschutzrechtlicher Sicht stellt sich die Sachlage so dar, dass das Thüringer Hochschulgesetz (ThürHG) zur Feststellung einer Prüfungsunfähigkeit an den Thüringer Hochschulen keine eigenen Regelungen enthält, sondern die Hochschulen nach § 49 Abs. 1 ThürHG fachübergreifende Bestimmungen für das Prüfungsverfahren (Rahmenprüfungsordnung) erlassen können. Der TLfDI schrieb daraufhin alle Thüringer Hochschulen an und bat um eine Darstellung des jeweils dort festgelegten Verfahrens zur Feststellung einer Prüfungsunfähigkeit. Die eingegangenen Antworten zeigten ein uneinheitliches Bild. Einigen Hochschulen reicht es zur Nachweisführung aus, wenn der Arzt auf einem von der Hochschule herausgegebenen Vordruck die Prüfungsunfähigkeit des Studierenden erklärt, während andere Hochschulen erheblich mehr Daten zum Gesundheitszustand des Prüfungskandidaten beim behandelnden Arzt erheben, etwa zur Einschätzung des Leistungsvermögens, zu den bestehenden Krankheitssymptomen bzw. der Art der Leistungsminderung sowie – als freiwillig gekennzeichnet – die Bezeichnung der Krankheit.

Gegen Verfahren derjenigen Hochschulen, die lediglich ein ärztliches Attest von Prüflingen verlangen, in dem der Arzt feststellt, dass der Prüfling wegen gesundheitlicher Beeinträchtigungen nicht an einer Prüfung teilnehmen kann, hat der TLfDI keine Bedenken. Bei den anderen Hochschulen, die vom behandelnden Arzt zusätzlich eine Beschreibung der gesundheitlichen Beeinträchtigungen verlangen, ist die Erforderlichkeit und Verhältnismäßigkeit dieser Datenerhebung von Krankheitsauswirkungen aus datenschutzrechtlicher Sicht nicht unmittelbar erkennbar. Die Hochschulen begründen die

Erforderlichkeit mit der Aufgabe der Prüfungsausschüsse, selbstständig über den Antrag in eigener Verantwortung darüber entscheiden zu müssen, ob im konkreten Fall eine Prüfungsunfähigkeit vorliegt. Darüber hinaus wurde auf einen Beschluss des Bundesverwaltungsgerichts vom 6. August 1996, Az.: 6 B 17.96 verwiesen. Darin stellte das Gericht hinsichtlich der Nachweisführung einer Prüfungsunfähigkeit in der ersten Juristischen Staatsprüfung fest, dass nicht der Arzt, sondern das Landesjustizprüfungsamt entscheidet, ob die nachgewiesenen Gründe es rechtfertigen, dass der Prüfling verhindert ist. Es gibt also eine höchstrichterliche Entscheidung darüber, welche formalen und inhaltlichen Anforderungen von der Prüfungsverwaltung an ein ärztliches Attest gestellt werden dürfen. Wenn eine Hochschule eine Satzung erlassen hat, in der bestimmt wird, in welcher Weise die Studierenden eine Prüfungsunfähigkeit gegenüber dem Prüfungsausschuss nachweisen müssen und sich der Umfang der verlangten gesundheitlichen Informationen in einem durch das oben genannte Urteil erforderlichen Datenumfang hält, so ist dieses zunächst auch aus datenschutzrechtlicher Sicht nicht zu beanstanden. Gegen Datenerhebungen, die im Umfang über den unbedingt erforderlichen Datenrahmen hinausgehen, wird der TLfDI aber von seiner Prüfkompetenz gegenüber den Hochschulen Gebrauch machen. In einer Hochschule wird das Verfahren zur Feststellung der Prüfungsunfähigkeit zurzeit einer Neubewertung unterzogen. Dies erfolgt in Abstimmung mit dem rechtsaufsichtlich zuständigen Ministerium für Wirtschaft, Wissenschaft und digitale Gesellschaft. Der TLfDI hat das Ministerium gebeten, ihn in das Verfahren mit einzubinden. Ergebnisse zum Verfahrensstand sind dem TLfDI noch nicht bekannt.

Zum Nachweis einer Prüfungsunfähigkeit sollte es den Hochschulen grundsätzlich genügen, wenn der Betroffene dem Prüfungsamt ein Attest vorlegt, in dem sein behandelnder Arzt die Prüfungsunfähigkeit bestätigt.

14.39 Erhebung von Täternamen bei sexueller Gewalt?

Im März 2010 hat das Bundeskabinett die Einrichtung des Runden Tisches „Sexueller Kindesmissbrauch in Abhängigkeits- und Machtverhältnissen in privaten und öffentlichen Einrichtungen und im familiären Bereich“ beschlossen. Die Mitglieder des Runden Tisches

hatten im November 2011 ihren Abschlussbericht verabschiedet. In diesem wurde unter anderem die Einrichtung eines Ergänzenden Hilfesystems (EHS) für diejenigen empfohlen, die in ihrer Kindheit bzw. Jugend sexuellen Missbrauch in der Familie oder in Institutionen erlitten haben und noch heute an diesen Folgewirkungen leiden. Der Bund stellte für den familiären Bereich 50 Mio. Euro bereit. Daher gibt es seit dem 1. Mai 2013 den „Fonds Sexueller Missbrauch im familiären Bereich". Aus Mitteln des Fonds können Betroffene Sachleistungen bis zum 30. April 2016 beantragen. Hierfür entwickelte der Bund ein einheitliches Antragsformular. Die Geschäftsstelle des „Fonds Sexueller Missbrauch im familiären Bereich" übernimmt die Entgegennahme sämtlicher Anträge und leitet diese an das zuständige Land weiter, wenn Gegenstand des Antrages ein Missbrauch in einer Institution des Landes ist. In diesem institutionellen Bereich übernehmen die Länder ihre Arbeitgeberverantwortlichkeit für Missbrauchsfälle, die durch Beschäftigte des Landes und der Kommunen zu verantworten sind.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ging davon aus, dass es im Verfahren für die Prüfung der Arbeitgeberverantwortung in der Vielzahl der Fälle notwendig sein würde, Informationen über den Täter zu erlangen. Dies ist aus Sicht des TLfDI aber nicht ohne Weiteres zulässig. Die zu erhebenden Daten sind sehr sensibel und nicht alle Betroffenen möchten wegen der damit verbundenen Folgen (z. B. der Notwendigkeit einer Aussage als Zeuge) den Täternamen benennen. Nach einer ersten Einschätzung des TLfDI kann eine Datenerhebung ausschließlich im Wege der Einwilligung der Betroffenen erfolgen. Es ist nicht erkennbar, dass die Datenerhebung des Täternamens für die Erfüllung der Aufgabe des EHS erforderlich ist. Diese besteht darin, „noch andauernde Belastungen als Folgewirkungen des Missbrauchs auszugleichen bzw. zu mildern", nicht aber in der Ermittlung und gegebenenfalls Sanktionierung der Täter.

An die Bestimmtheit einer derartigen Einwilligungserklärung und die Darstellung der mit der Datenverarbeitung verfolgten Zwecke sind besonders hohe Anforderungen zu stellen. In jedem Einzelfall ist eine strenge Erforderlichkeitsprüfung notwendig. Der TLfDI setzte sich Anfang des Jahres 2015 mit dem zuständigen Ressort in Verbindung, um zu erfahren, in welcher Weise eine Umsetzung des EHS für den institutionellen Bereich im Freistaat Thüringen erfolgen und wie das Verfahren der Prüfung der Arbeitgeberverantwortung

ausgestaltet werden soll. Dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) wurde mehrmals Fristverlängerung gewährt. Dieses teilte noch im Mai 2015 mit, zwischen den Ländern habe sich Diskussionsbedarf entwickelt und die notwendigen Beschlüsse und Vereinbarungen lägen noch nicht vollständig vor. Es war nicht in Erfahrung zu bringen, bis wann mit einer Antwort auf die vom TLfDI gestellten Fragen zu rechnen ist. Nach § 38 Abs. 1 Nr. 1 ThürDSG sind der Landesbeauftragte für den Datenschutz und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis insbesondere Auskunft zu ihren Fragen zu gewähren. Unter Hinweis auf diese Unterstützungspflicht aller öffentlichen Stellen in Thüringen gegenüber dem TLfDI wandte sich dieser an die zuständige Abteilung des TMBJS. Bis zum Ende des Berichtszeitraums ging beim TLfDI keine Antwort ein. Der TLfDI wird die Angelegenheit weiterverfolgen und eine Beanstandung wegen mangelnder Unterstützung des TLfDI androhen. Über den Ausgang des Verfahrens wird im nächsten Tätigkeitbericht informiert werden.

Nach § 38 Abs. 1 Nr. 1 ThürDSG sind der Landesbeauftragte für den Datenschutz und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Die Erfüllung der Beantwortungspflicht erleichtert dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit die Wahrnehmung seiner Kotrollaufgabe. Nur wenn er alle notwendigen Informationen enthält, kann er die Einhaltung datenschutzrechtlicher Vorgaben prüfen.

14.40 Lehrer-Apps: kritisch

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat in seiner Eigenschaft als Vorsitzender der Unterarbeitsgruppe des Arbeitskreises Datenschutz und Bildung der Datenschutzbeauftragten das Thema des Einsatzes von Apps auf privaten IT-Systemen von Lehrern aufgegriffen und erstellt zurzeit gemeinsam mit anderen Landesdatenschutzbeauftragten in dieser Arbeitsgruppe ein Informationsblatt, welches sich an Schulleiter und Lehrkräfte richtet und die einschlägigen datenschutzrechtlichen Vorschriften darstellen sowie die erforderlichen technischen und organi-

satorischen Maßnahmen erläutern soll, die von den Lehrkräften zu ergreifen sind, um Schüler-, Eltern- und Lehrerdaten zulässigerweise mit Mobilgeräten verarbeiten und nutzen zu können. Im Rahmen der weiten Verbreitung von mobilen Datenverarbeitungsgeräten, wie Smartphones, Tablets und Notebooks, besteht bei den Lehrkräften das Bedürfnis, diese in erster Linie für die private Nutzung vorgesehenen Geräte auch für ihre dienstliche Arbeit einzusetzen. Der Einsatz von im privaten Besitz befindlichen Geräten zu dienstlichen Zwecken wird auch als „bring your own device“ (BYOD) bezeichnet. In Thüringen gibt es, wie in den meisten anderen Bundesländern, bislang noch keine Vorschriften, die speziell die dienstliche Nutzung von privaten, mobilen Endgeräten regeln. Da die vorhandenen Thüringer Vorschriften zur Verarbeitung personenbezogener Daten von Schülern auf privaten Rechnern der Lehrkräfte bereits vor 15 Jahren erstellt wurden, beziehen sich diese ausschließlich auf die Verwendung des heimischen stationären PC. Es ist davon auszugehen, dass trotz fehlender rechtlicher Voraussetzungen die dienstliche Nutzung von mobilen Endgeräten durch Lehrkräfte durchaus verbreitet ist oder zumindest ins Auge gefasst wird. Die Privatwirtschaft stellt für die dienstlichen Bedürfnisse der Lehrerinnen und Lehrer eine immer mehr anwachsende Zahl von „Lehrer-Apps“ (App ist die Abkürzung für das englische „Application“ und meint eine Anwendersoftware) zur Verfügung, die das bisherige „Notenbüchlein“ oder den Terminkalender in Papierform ersetzen. Die Funktionalitäten und Verwendungsmöglichkeiten gehen dabei weit über die bisherige analoge Verarbeitung und Nutzung von personenbezogenen Schüler-, Eltern- und Lehrerdaten hinaus. Neben der Leistungsfähigkeit der Apps haben Mobilgeräte auch den Vorteil, diese ständig mit sich führen zu können und unabhängig von einem festen Arbeitsplatz Schülerdaten verarbeiten und nutzen zu können. Allerdings ergeben sich aus den genannten Vorteilen von Mobilgeräten auch zahlreiche datenschutzrechtlich relevante Sicherheitsprobleme. Dies fängt an bei der Gefahr, die kompakten und ständig im mobilen Gebrauch befindlichen Geräte zu verlieren und geht über nicht genutzte Sicherheitseinstellungen, ungeprüft installierte Apps bis hin zur unkritischen Verwendung des Gerätes in der Öffentlichkeit. Der TLfDI wird nach der Fertigstellung des Informationsblatts dieses den Lehrkräften über die Schulen zukommen lassen.

Die Verwendung von privaten mobilen Geräten durch Lehrkräfte zu schulischen Zwecken ist aus datenschutzrechtlicher Sicht kritisch zu sehen und erfordert das Ergreifen zahlreicher technischer und organisatorischer Maßnahmen, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Mit einem hierfür erarbeiteten Informationsblatt wird der TLfDI die Lehrerschaft auf die bestehenden Gefahren hinweisen und Lösungsmöglichkeiten beschreiben.

Online Security Technology © GKSD / Fotolia.com

15 Entwicklungen der automatischen Datenverarbeitung

15.1 Verschlüsselung mit TrueCrypt

Lange galt TrueCrypt als sicheres Programm zum Verschlüsseln von Daten auf der Festplatte, auf Datenträgern oder aber auch zum Verschlüsseln der Daten vor einer Datenübermittlung. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl dieses Programm. Doch die Weiterentwicklung dieses Programms wurde durch die Entwickler Ende Mai 2014 eingestellt, sodass nunmehr keine Empfehlung seitens des BSI mehr erfolgt.
Da einige Programmteile von TrueCrypt auch in anderen Programmen verwendet werden, hatte das BSI das Fraunhofer-Institut für sichere Informationstechnologie (SIT) mit der Durchführung einer Sicherheitsanalyse von TrueCrypt in der Version 7.1a beauftragt. Das Ergebnis dieser Sicherheitsanalyse wurde vom BSI im November 2015 unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2 veröffentlicht.

In der Studie wird u. a. festgestellt, dass TrueCrypt nur dann noch einen wirksamen Schutz entfaltet, wenn das Gerät, auf dem die Daten gespeichert sind, sich im ausgeschalteten Modus befinden. Dies ist bspw. bei Verlust des USB-Sticks oder Laptops der Fall.
Die Studie kommt zum Schluss, dass in den anderen Fällen, also bspw. im Online-Modus, kein sicherer Schutz mehr besteht. Grund dafür ist, dass der Einsatz eines heimlich installierten Key-Logger-Programms, also eines Programms, welches die Eingabe an der Tastatur mitschneidet, den Schutz unterlaufen könnte. Ebenso kann andere installierte Schadsoftware den Schutz von TrueCrypt unterlaufen.
Was bedeutet dies nun für die Anwender? Wieso wird hier auf einmal die Gefahr des Key-Loggers problematisiert und bei anderen sicherheitsrelevanten Prozessen bewusst ausgeblendet?
Die Datenschutzbeauftragten des Bundes und der Länder haben beispielsweise bei der Einführung des elektronisch lesbaren Personalausweises die unsicheren Lesegeräte ohne eigenständige Tastatur genau aus diesem Grund kritisiert und vor Key-Loggern gewarnt. Weder die Bundesregierung noch das BSI änderten daraufhin das Verfahren dahingehend, dass nur Lesegeräte mit eigener Tastatur zugelassen werden.
Auch darf der Bürger sich fragen, wenn er die von der Bundesregierung favorisierte De-Mail benutzt (siehe Nummer 5.51), ob diese vor einem Key-Logger geschützt ist. Diesbezügliche Aussagen sind für den Bürger derzeit nicht zu finden.
Welche Alternative schlägt nun das BSI hinsichtlich TrueCrypt vor? Muss man gänzlich auf TrueCrypt verzichten? Aus datenschutzrechtlicher Sicht ergibt sich aus der vorliegenden Sicherheitsanalyse, dass TrueCrypt durchaus weiter Anwendung finden kann, wenn die Daten auf einem Gerät nur bei Verlust oder Diebstahl des Gerätes vor unberechtigtem Zugriff gesichert werden sollen. Auch für ausgelagerte Datensicherungen scheint es gemäß der oben zitierten Studie des Fraunhofer-Instituts weiterhin geeignet. Nur für den Zugriff auf Daten in laufenden Systemen kann die Verschlüsselung allein keinen ausreichenden Schutz gewährleisten.
Man muss also vor dem Einsatz immer schauen, welche Empfehlungen derzeit das BSI ausspricht (https://www.bsi.bund.de/DE/Home/home_no

de.html). Wichtig ist, dass man immer dem Stand der Technik entsprechende Verschlüsselungssoftware einsetzt, um nicht fahrlässig zu handeln.

Verschlüsselungssoftware ist immer entsprechend dem aktuellen Stand der Technik einzusetzen. Daher sollte man sich regelmäßig beim Bundesamt für Sicherheit in der Informationstechnik (BSI) informieren.

15.2 Ein Schritt vor, zwei zurück – ist die Verschlüsselung politisch wirklich gewollt?

Durch die zunehmende digitale Vernetzung und die Erkenntnis, dass Sicherheitsbehörden heimlich Daten abgreifen und die Wirtschaftsspionage zunimmt, gewinnt die Verschlüsselung von Daten bei der Datenübermittlung und Datenspeicherung verstärkt an Bedeutung.
Das Sicherheitsbedürfnis, dass nur Befugte Daten zur Kenntnis nehmen sollen, haben Bürger, Unternehmen und auch die öffentliche Verwaltung. Insbesondere Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie z. B. Ärzte, Anwälte, Psychologen und Steuerberater, müssen die Vertraulichkeiten der Daten gewährleisten. Aber auch Journalisten und Abgeordnete haben großes Interesse daran, dass sich jedermann vertraulich an sie wenden kann.
Wie wichtig eine zuverlässige und sichere Verschlüsselung von Daten ist, hatte auch die Bundesregierung im Dokument „Digitale Agenda 2014-2017“ deutlich gemacht.

So heißt es in der Agenda:

> „Ohne Vertrauen in die Sicherheit und Integrität der digitalen Welt wird es nicht gelingen, die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen. Das Vertrauen zu stärken heißt daher zum einen, die Kommunikation über digitale Netze zu schützen und dafür den Zugang zu sicheren und einfach zu nutzenden Verschlüsselungsverfahren zu fördern.
> Zum anderen bedeutet es, dass wir unsere kritischen Infrastrukturen schützen. Wir wollen mit der Digitalen Agenda einen wesent-

lichen Beitrag dazu leisten, dass unser Land einer der sichersten digitalen Standorte weltweit bleibt."

„Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungs-Standort Nr. 1 auf der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

„Wir fördern und fordern den Einsatz von vertrauenswürdigen IT-Sicherheitstechnologien, insbesondere von mehr und besserer Verschlüsselung in der elektronischen Kommunikation."

Das war allerdings im August 2014.

Im Zusammenhang mit dem Anschlag in Paris am 7. Januar 2015 wurde dann sofort seitens der Politik über die Notwendigkeit einer Schwächung von Verschlüsselungstechnologien diskutiert, um so dem Terrorismus wirksam zu begegnen.

So konnte man schon im gleichen Monat einer Meldung bei http://www.heise.de/ entnehmen, dass – neben dem britischen Premiers David Cameron und US-Präsident Obama – auch der Bundesinnenminister Thomas de Maizière nun Zugang zu verschlüsselten Daten wünscht. So forderte er, dass deutsche Sicherheitsbehörden befugt sein und in die Lage versetzt werden müssen, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen, wenn dies für ihre Arbeit und zum Schutz der Bevölkerung notwendig ist.

Aus diesem Grund wendete sich im März 2015 die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer ihrer Entschließungen an die Politik und forderte sie auf, sich aktiv für das Brief-, Post- und Fernmeldegeheimnis und bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschrän-

ken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich (siehe Anlage 23).

Kryptographische Verfahren dienen der Gewährleistung der Vertraulichkeit und Integrität. Insbesondere ist eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeit Dritter bereitzustellen. Kryptographische Verfahren durch staatliche Regulierungen zu unterbinden, würde unter Umständen auch dem Brief-, Post- und Fernmeldegeheimnis entgegenwirken.

15.3 Betriebssysteme mit Cloud-Anbindung – immer online

„Daten in der Cloud“ sind in aller Munde und unsere Gesellschaft hat diesen Begriff in den täglichen Gebrauch aufgenommen. Doch was ist eine Cloud und was hat sie mit Betriebssystemen zu tun?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete bereits im 10. Tätigkeitsbericht (Punkt 14.4) über die Risiken des Cloud Computing. Allgemein gesprochen ist die „Cloud“ ein Ersatzkonstrukt, welches Datenspeicherung und -verarbeitung von lokalen Geräten wie PCs, Laptops, Tablets und auch Smartphones in den Bereich des Internets auslagert. Der Nutzer erfährt gar nicht mehr, wo genau seine Daten gespeichert sind. Und genau dieses unscharfe Wissen, „wo“ „was“ verarbeitet wird, prägt den Begriff der Cloud (oder auch der Wolke). Die Vorteile liegen für den Nutzer dabei auf der Hand: Er muss sich nicht um Details kümmern. So ist es normal geworden, von überall Zugang zu Mails, Kurznachrichten, Kartendiensten oder Sprachassistenten zu haben. Auch Fotos und Musikbibliotheken werden zunehmend nicht mehr auf dem Gerät, sondern in der Cloud gespeichert, damit sie von überall und auch mittels verschiedener Geräte abrufbar sind. Aber auch Unternehmen und öffentliche Stellen nutzen vermehrt Cloud-Dienste bewusst oder unbewusst.
Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste und der Wirtschaftsspionage empfahl der TLfDI, bei der Nutzung von Cloud-Diensten generell deutsche oder europäische Cloud-Anbieter

vorzuziehen, die zudem von vertrauenswürdigen Stellen zertifiziert sind (10. Tätigkeitbericht Pkt. 14.4).
Nachfolgend wird hier nun insbesondere die neue Entwicklung der Integration von Cloud-Funktionen in Betriebssystemen behandelt und auch auf die Änderungen der Orientierungshilfe Cloud Computing V2.0 eingegangen.
Aus der Sammlung und Aufbereitung von Datenspuren zur Bildung von Personenprofilen ist in den letzten Jahren ein großer Markt entstanden, und von diesem Markt wollen die großen Hersteller von Betriebssystemen nun auch profitieren. Bisher stellten Betriebssysteme Grundfunktionen wie Speichern und Laden von Daten, Ausführen von Programmen auf dem Gerät und die Kommunikationsmöglichkeit mit anderen Geräten zur Verfügung. Einige Betriebssystemhersteller bieten nun zum Teil auch schon Online-Funktionen wie die Internetsuche über Sprachbefehle, zentrale Terminplaner, Kartendienste oder das Speichern von Daten auf einem Speicherplatz „in der Cloud“ an. Dadurch kann das Verhalten der Benutzer von ihnen besser nachvollzogen und im Detail analysiert werden. Leider unterliegen die Betriebssystemanbieter dabei oft nicht dem deutschen oder europäischen Datenschutzrecht.

Aus datenschutzrechtlicher Sicht bergen cloud-unterstützte Betriebssysteme generell Datenschutzrisiken. Einer der Kritikpunkte sind dabei die Standardeinstellungen. Diese sind meist so gewählt, dass der Betriebssystemhersteller schon bei der ersten Inbetriebnahme sehr viele Daten erfasst. Das Datenschutzprinzip, dass die Standardeinstellungen bei der Inbetriebnahme des Systems vom Hersteller so gewählt werden, dass möglichst wenig Daten übermittelt werden (Privacy-by-Default), wird hier weitestgehend ignoriert.

Das Fenster zur Privatsphäre ist somit geöffnet. So konnte man im August 2015 der Fachpresse entnehmen, dass nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten sofort an Microsoft übertragen werden. Außerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich“ angesehen wird (siehe dazu: http://www.microsoft.com/de-de/privacystatement/default.aspx).

Aus diesem Grund hatte der TLfDI noch im gleichen Monat eine entsprechende Pressemitteilung veröffentlicht: (https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pressemitteilung_windows_10.pdf).

In dieser wurde auf die Notwendigkeit hingewiesen, selbst noch persönliche Einstellungen vorzunehmen, um die eigene Privatsphäre zu schützen. Dabei wurde gleich ein entsprechender externer Link zu Tipps zur Verbesserung der Einstellungen bei Windows 10 veröffentlicht. Dadurch konnten Bürger zeitnah durch Selbsthilfe ihr Betriebssystem datenschutzgerechter einstellen.

Auch die 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahm sich dann im Oktober 2015 des Themas der cloud-unterstützten Betriebssysteme an und zeigte in der Entschließung „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ die entsprechenden Datenschutzrisiken auf (siehe dazu Anlage 30).

So können nach Angaben der Konferenz weitreichende Datenverarbeitungsbefugnisse nicht dadurch gerechtfertigt werden, dass Nutzer auf Basis der Zustimmung zu AGB datenschutzunfreundlichen Voreinstellungen implizit zustimmen würden. Auch das Ermöglichen einer Opt-Out-Lösung wird nicht als zielführend angesehen, d.h. das manuelle Abschalten der Dienste im Nachhinein ist keine datenschutzfreundliche Lösung. Systeme dürfen nicht einfach Daten erfassen und im Nachhinein fragen, ob man es nicht will, sondern müssen

vorab fragen, ob man dieser Datenerfassung zustimmt (Opt-In-Lösung). Hier bedarf es technisch unterstützter Einwilligungslösungen, die vor der Inbetriebnahme greifen müssen. Für jeden Dienst muss theoretisch eine Einwilligung (und auch die Möglichkeit des Widerrufs) gegeben werden. Der Widerruf ist momentan nur durch das Finden und Nutzen der entsprechenden Einstellungen möglich und damit ein sehr mühsamer Weg. Die Konferenz fordert daher die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Weiterhin empfiehlt die Datenschutzkonferenz in der oben genannten Entschließung den Benutzern der neuen Betriebssysteme, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen.

Moderne Betriebssysteme bieten heutzutage viele Cloud-Funktionalitäten an. Dabei sind die Standardeinstellungen selten datenschutzgerecht; Privacy-by-default wird daher nicht umgesetzt. Der Nutzer muss sich momentan selber behelfen und durch Recherche die möglichen Einstellvarianten finden. Der rechtliche Mechanismus der Einwilligung und des Widerrufs ist technisch noch unzureichend umgesetzt und zu kompliziert. Damit sind viele Betriebssysteme heute Datenschleudern-by-default.

15.4 Problem: Biometrische Gesichtserkennung

Biometrische Gesichtserkennungen sind auf dem Vormarsch. Für diesen Zweck müssen vom Gesicht des Nutzers Merkmale berechnet werden, welche beim ersten Erkennungsvorgang dann einer Person zugeordnet werden. Diese erfassten biometrischen Merkmale bilden danach die Grundlage für eine spätere Wiedererkennung. Der Trend geht bspw. dahin, dass man sich mit dieser dann an Geräten anmelden kann, indem bei der jeweiligen Technik-Anmeldung das Gesicht erneut erfasst und mit den bereits gespeicherten biometrischen Merkmalen verglichen wird. Ist der Vergleich positiv, erfolgt die Anmeldung nutzerbezogen am Gerät.
Pech für den, der gerade eine Gesichts-OP hatte oder wenn eine andere Person unberechtigt vom Berechtigten, bspw. im Schlaf oder im Vollrausch, vor dem jeweiligen Gerät diese Funktion auslöst, um

den unberechtigten Zugang bspw. zum Handy und den darauf gespeicherten Mails zu bekommen.
Aber Spaß beiseite!
Die Gesichtserkennung ist unter anderem auch geeignet, Begehrlichkeiten beim Arbeitgeber zu wecken, den Zugang zu sensiblen Bereichen per Gesichtserkennung zu regeln und kontrollieren zu können. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte schon am 23. Mai 2013 in der Pressemitteilung „Nur mit dem Fingerabdruck zum Arbeitsplatz?“ darauf hingewiesen, dass die Erhebung, Speicherung und Verwendung biometrischer Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der ArbeitnehmerInnen darstellt, der datenschutzrechtlich nicht gerechtfertigt ist. Nur in besonderen Einzelfällen kann eine biometrische Zutritts- oder Zugriffskontrolle am Arbeitsplatz unter strengen Voraussetzungen zulässig sein.
Aus datenschutzrechtlicher Sicht haben alle oben genannten Beispiele gemeinsam, dass sich Nutzer überlegen sollten, ob sie diese Funktionalität wirklich selbst wollen oder lieber darauf verzichten sollten. In ihren Überlegungen sollten sie auch prüfen, ob die biometrischen Merkmale verschlüsselt abgespeichert und vor unberechtigtem Zugriff Dritter geschützt sind.
Biometrische Gesichtserkennungen werden aber auch in sozialen Netzwerken zunehmen. Schon jetzt ist es üblich, dass man bspw. bei (Gruppen-)Fotos eine Person markieren und dieser Markierung einen bestimmten Namen zuweisen kann. Es gibt auch bereits Software, die aufgrund einer Markierung auf einem Foto dann den ganzen Datenbestand durchsuchen kann, auf welchen Fotos diese Person noch zu sehen ist. Im privaten Hausgebrauch scheint dies auch eine nützliche Software. Diese Funktionalität – dann von Betreibern sozialer Netzwerke in ihren sozialen Netzwerken eingesetzt – bietet allerdings die Möglichkeit einer Komplettdurchsuchung über alle gespeicherten Fotos in der Datenbank des sozialen Netzwerkes. Sowohl für die Profilbildung, die Betreiber sozialer Netzwerke gerne für ihre eigenen Interessen optimieren wollen, als auch für jegliche Sicherheitsbehörden können solche Gesichtserkennungsprogramme hochinteressant werden.
Aus diesem Grund hatte die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2014 in einer Entschließung „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“ auch noch

einmal auf die erforderliche Einwilligungserklärung des Betroffenen hingewiesen (siehe dazu Anlage 6). Eine der wichtigsten Forderungen ist, dass über jegliche biometrische Gesichtserkennung der Betroffene in der Regel vorher informiert wird und sie nur mit Einwilligung des Betroffenen erfolgen darf.

Eine biometrische Gesichtserkennung zur Zugangskontrolle zu Geräten und zu Räumen scheint auf den ersten Blick eine optimale Lösung, bedarf aber einer vorhergehenden Einwilligung des Betroffenen. Auch soziale Netzwerke haben die Vorteile der Gesichtserkennung für ihre Zwecke erkannt. Aber auch hier bedarf es in jedem Fall der vorhergehenden Einwilligung des Betroffenen. Weiterhin sind die gespeicherten biometrischen Merkmale verschlüsselt zu speichern und der Zugriff von Dritten ist auszuschließen.

15.5 Verschlüsselung hilft nicht immer – auf die inneren Werte kommt es an

Im Frühjahr 2014 wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von einem Bürger darauf aufmerksam gemacht, dass beim Thüringer Landesamt für Statistik eine Webseite zur Beantragung von Wahlscheinen zwar verschlüsselt, dort jedoch nur ein veralteter Verschlüsselungsalgorithmus unterstützt würde. Da auf diesem Teil der Webseite Wahlscheine zur Kommunal- und Europawahl beantragt werden konnten, sind dort durchaus persönliche Daten erfasst worden.
Gemeinhin ist es so, dass der Nutzer beim Surfen im Internet die Nutzung von Verschlüsselung am Kürzel „https://“ oder an diversen Schlosssymbolen im Browser erkennt. Dies sagt allerdings nur aus, dass überhaupt eine Verschlüsselung stattfindet und, wenn keine weiteren Warnhinweise angezeigt werden, dass der Browser der Webseite vertraut. All das traf auch auf diesen Fall zu; aber dennoch war die Verschlüsselung nicht sicher. Warum? Dazu muss man auch wissen, dass es nicht nur einen Verschlüsselungsalgorithmus gibt, der durch HTTPS unterstützt wird, sondern mehrere. Beim Verbindungsaufbau zu einer verschlüsselten Seite schickt der Rechner des Nutzers eine Liste der unterstützten Algorithmen und welche in welcher Reihenfolge präferiert werden sollten. Der Server sucht sich dann den ersten passenden Algorithmus aus, den er unterstützen kann. Dieses Schema ist notwendig, um eine maximale Flexibilität

und Kompatibilität zu erreichen. Von diesem Prozess merkt der Nutzer für gewöhnlich nichts. Die Untersuchung des TLfDI ergab nun, dass der Webserver vom Thüringer Landesamt für Statistik ausschließlich den RC4-Algorithmus zur Verschlüsselung unterstützte. Dieser gilt durch die NSA als in Echtzeit knackbar (siehe http://www.heise.de/security/meldung/NSA-entschluesselt-Webserver-Daten-angeblich-in-Echtzeit-2041383.html) und wird daher auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als unsicher eingestuft.

Auf diesen Missstand machte der TLfDI die zuständigen Behörden – das Landesamt für Statistik und das Thüringer Landesrechenzentrum – aufmerksam und es erfolgte eine Umstellung auf zurzeit als sicher geltende Verschlüsselungsverfahren.

Nicht jede verschlüsselte Verbindung ist auch automatisch sicher. Die Sicherheit hängt maßgeblich vom verwendeten Algorithmus ab. Unglücklicherweise bemerkt man als Nutzer nicht, welcher Algorithmus verwendet wird, sodass dies eine Sicherheitslücke darstellen kann. Glücklicherweise konnte der TLfDI diese in diesem Fall beseitigen lassen. Für Hinweise zu anderen Fällen ist der TLfDI weiterhin dankbar.

15.6 Ein neues „Labor“ beim TLfDI – Prüfung von Apps

Die Welt der Informationstechnik entwickelt sich in einem schnellen Tempo weiter, und ebenso nimmt auch die Vernetzung in unterschiedlichsten Bereichen weiter zu. Vor allen Dingen Smartphones und Tablets sind heutzutage die täglichen Kommunikationswerkzeuge und als solche in der Regel dauerhaft mit dem Internet verbunden. Diese werden unter anderem zum Empfangen und Senden von Nachrichten, zum Surfen im Internet, zum Buchen von Fahrkarten oder für Online-Spiele genutzt. Dies geschieht über Apps. Viele Anwendungsbereiche erfreuen sich zunehmend solcher App-Anwendungen. So werden bspw. von Universitäten, Bibliotheken, Verkehrsbetrieben, Tourismusbranchen und Stadtwerken Apps für alle möglichen Anwendungsgebiete angeboten. Auch im Gesundheitsbereich sind zunehmend Apps im Einsatz (siehe dazu Nr. 11.8).

Aus datenschutzrechtlicher Sicht ist dabei von Interesse, welche Daten diese Apps erfassen und wohin die Daten wie versendet werden.
Die Apps dabei ausschließlich aus der verfügbaren Dokumentation heraus datenschutzrechtlich zu beurteilen, ist dabei nicht zuverlässig möglich. Oft liegen nicht einmal diesbezügliche Dokumentationen vor. Deshalb hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) 2015 ein neues „Prüflabor“ für Apps in Betrieb genommen. Vorbild ist dabei das Prüflabor beim Bayerischen Landesamt für Datenschutzaufsicht. Mit dem Prüflabor beim TLfDI, derzeit ein eigenständiger eingerichteter Arbeitsplatz, ist es nun möglich, Apps z. B. von Endgeräten wie Smartphones, Tablets, Laptops oder anderen netzwerkfähigen Geräten zu analysieren. Das Labor basiert vor allen Dingen auf frei verfügbaren Open-Source-Lösungen auf Linux-Basis und Eigenentwicklungen.
Nach der Inbetriebnahme erfolgten im Laufe des 2. Halbjahres 2015 erste technische Untersuchungen von Apps. Hierbei konzentriert sich der TLfDI entsprechend seiner Zuständigkeit auf Apps, die von Thüringer Behörden und Unternehmen eingesetzt werden. Neben der technischen App-Prüfung bedarf es allerdings auch einer rechtlichen Bewertung. Eine abschließende datenschutzrechtliche Bewertung von Apps ist besonders in den Fällen aufwendig und dauert unter Umständen einige Wochen, in denen App-Hersteller Programmteile nutzen, deren genaue Funktionsweise sie selbst nicht genau kennen.

Der TLfDI hat sich entsprechend seiner Zuständigkeit vorgenommen, Apps, die von Thüringer Behörden und Unternehmen eingesetzt werden, technisch und datenschutzrechtlich zu prüfen. Dies ist ein sehr zeit- und personalaufwändiger Prozess. Dennoch ist der TLfDI über jeden Hinweis auf solche Apps dankbar.

15.7 IT-Sicherheitsgesetz nicht ohne Datenschutz!

Seit den Terroranschlägen vom 11. September 2001 sind neben der Informationstechnik auch „kritische Infrastrukturen“ in den Mittelpunkt staatlicher Sicherheitsvorsorge gerückt. Im Jahr 2009 veröffentlichte das Bundesinnenministerium des Innern die „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“. Im Jahr 2011 folgte die „Cyber Sicherheitsstrategie für Deutschland“, in der die Bundesregierung darauf hinwies, dass u. a. die Ver-

fügbarkeit des Cyber-Raums die existenzielle Frage des 21. Jahrhunderts geworden sei. Wirtschaft und Bevölkerung seien auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen. Der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum könnten nach Angaben der Bundesregierung zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen.

Ein nationales Cyber-Abwehrzentrum wurde geschaffen, mit dem Ziel, die operative Zusammenarbeit der relevanten staatlichen Stellen zu optimieren und die Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle zu koordinieren.

Anfang 2013 wurde dann vom Bundesministerium des Innern ein Referentenentwurf eines IT-Sicherheitsgesetzes zur Diskussion veröffentlicht, welcher eine Reihe von Kritik erfuhr.

Anfang Januar 2015 ereignete sich das Attentat auf die Redaktion „Charlie Hebdo“ in Paris. Mit dem Attentat begann nun auch wieder eine verschärfte politische Diskussion zur Sicherheit Deutschlands.

Ende Februar 2015 brachte die Bundesregierung dann den Gesetzentwurf für ein IT-Sicherheitsgesetz ein, um die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern.

Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die ausdrücklich die Notwendigkeit von Informationssicherheit befürwortet, kritisierte in ihrem entsprechenden Entschluss im März 2015 diesen Gesetzentwurf sehr scharf (siehe https://www.tlfdi.de/tlfdi/berichte/entschliessungen_datenschutzkonferenz/89/).

So seien beispielsweise die neuen Melde- und Benachrichtigungspflichten bei erheblichen IT-Sicherheitsvorfällen an das Bundesamt für Informationstechnik (BSI) nicht mit einer datenschutzrechtlichen Meldepflicht bei Datenpannen an die Datenschutzaufsichtsbehörden verbunden. Weiterhin kritisierte die Konferenz, dass zu unklar sei, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welchen Zweck erhoben, verarbeitet und gespeichert werden dürfen.

Wie der Zufall es so wollte: Während der Bundestag über dieses Gesetz diskutierte und dieses Gesetz dann auch verabschiedete, ereilte das Bundestagsnetzwerk selbst ein Cyberangriff. Das IT-Sicherheitsgesetz trat, nun fast logisch, dann am 25. Juli 2015 in Kraft (Bundesgesetzblatt Teil 1 Nr. 31 vom 24. Juli 2015). Es schreibt die Einhaltung eines Mindestniveaus an IT-Sicherheit und von Meldepflichten bei Betreibern so genannter kritischer Infrastrukturen vor. Als kritische Infrastrukturen werden dabei gesehen: Einrichtungen, Anlagen oder Teile, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und zugleich von hoher Bedeutung für das funktionierende Gemeinwesen sind. Nach Angaben des Gesetzes sollen Einzelheiten zum Anwendungsbereich und zum Adresskreis noch in einer Rechtsverordnung bestimmt werden.
Mit dem IT-Sicherheitsgesetz wurde auch das Telekommunikationsgesetz geändert und die rechtliche Möglichkeit geschaffen, dass Telekommunikationsdiensteanbieter die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer bei Erforderlichkeit erheben und verwenden dürfen, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.
Interessanterweise erfolgte, um ein paar Monate zeitversetzt, das parlamentarische Gesetzgebungsverfahren zum „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“, welches im Oktober 2015 vom Bundestag bestätigt wurde (siehe dazu Nr. 2.1). Man erkennt unweigerlich, dass der Bedarf, die Informationstechnik zu schützen und insbesondere Terroristen zu überwachen, offenbar zunimmt. Dies darf aber immer nur in ausgewogener Balance zum Datenschutz erfolgen. Die Datenschutzbeauftragten werden daher auch weiter darum kämpfen, dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren. Die Datenschutzbeauftragten werden daher weiter darum kämpfen,

dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

15.8 Happy Birthday – die elektronische Gesundheitskarte wird 10 Jahre alt

Bereits im November 2003 wurde das „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung“ (GKV-Modernisierungsgesetz – GMG) erlassen. Dies hatte zur Folge, dass auch das Sozialgesetzbuch (SGB) Fünftes Buch (V) u. a. in § 291 und § 291a geändert wurde. So wurde damals festgelegt, dass die Krankenversichertenkarte bis spätestens zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte zu erweitern ist. Auch wurde festgelegt, welche Daten die elektronische Gesundheitskarte beinhalten muss und welche Daten wie verarbeitet werden sollen.
Der Thüringer Landesbeauftragte für den Datenschutz berichtete in seinen Tätigkeitsberichten mehrfach darüber.
Allerdings ist die elektronische Gesundheitskarte erst seit dem 1. Januar 2015 Pflicht und gilt seit diesem Zeitpunkt bundesweit ausschließlich als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkassen beim Arzt oder Zahnarzt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte daraufhin zum aktuellen Sachstand in einer Pressemitteilung (siehe dazu Anlage 47).
Seit dem 29. Dezember 2015 ist nun auch das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze in Kraft (E-Health-Gesetz). So soll nun mittels der elektronischen Gesundheitskarte die Verbesserung der Wirtschaftlichkeit, Qualität und Transparenz der Behandlung durch moderne Anwendungen und Informations- und Kommunikationstechnologien erzielt werden (siehe dazu Nr. 11.7).
Damit auch die kommenden Anwendungen in Thüringen datenschutzrechtskonform umgesetzt werden, hat der TLfDI seine Gesprächsbereitschaft gegenüber der Landesärztekammer Thüringen und der Landesapothekerkammer Thüringen bekundet.
Unabhängig davon wird der TLfDI den weiteren Werdegang dieser Karte aufmerksam verfolgen.

Der Einsatz der elektronischen Gesundheitskarte wird auch künftig vom TLfDI kritisch beobachtet. Der TLfDI bittet daher um Hinweise, falls datenschutzrechtliche Probleme auftauchen.

15.9 Cloud-Computing 2.0 und Safe Harbor

Zur datenschutzkonformen Gestaltung und zur Nutzung von Cloud-Computing hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits 2011 eine Entschließung veröffentlicht. Damals wurde parallel zur Entschließung auch eine entsprechende Orientierungshilfe (OH) erarbeitet (siehe 9. TB, Pkt. 14.1). Diese Orientierungshilfe richtet sich sowohl an die Anbieter von Cloud-Diensten als auch an deren Nutzer.

Aufgrund der technischen Entwicklung und aufgrund der NSA-Affäre wurde sie drei Jahre später überarbeitet und 2014 unter „Cloud-Computing 2.0“ veröffentlicht:
https://www.tlfdi.de/imperia/md/content/datenschutz/themen/orientierungshilfen/oh_cc_2.0.pdf.

Die OH „Cloud-Computing 2.0“ geht nun neben dem grenzüberschreitenden Datenverkehr auch auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA) ein. Es wird darauf hingewiesen, dass es für die Zugriffsbefugnisse der US-Behörden nicht maßgebend ist, ob sich die Cloud innerhalb oder außerhalb der USA befindet. Es wird nach US-Recht als ausreichend angesehen, wenn der Cloud-Anbieter zumindest auch in den USA geschäftlich tätig ist.

Aus datenschutzrechtlicher Sicht steht eine entsprechende Datenübermittlung von Unternehmen mit Sitz in Europa bzw. Deutschland an US-Behörden nicht mit Art. 26 der Richtlinie 95/46/EG bzw. § 4c BDSG im Einklang. Zudem würde bei einer entsprechenden Datenübermittlung durch den Cloud-Anbieter auch der Cloud-Anwender automatisch gegen europäisches und deutsches Datenschutzrecht verstoßen, da er in seiner datenschutzrechtlichen Verantwortlichkeit bleibt. Letzteres ergibt sich aus der Tatsache, dass bei Auftragsdatenverarbeitung der Auftraggeber verantwortliche

Stelle bleibt. Die OH weist deshalb darauf hin, dass derzeit ein internationales Übereinkommen fehle, welches eine solche Datenübermittlung an US-Behörden rechtfertige.
Auch in den USA ansässige Cloud-Anbieter, die sich dem Safe-Harbor-Abkommen zwischen der EU und den USA angeschlossen hatten, waren von diesem staatlichen Eingriff durch US-Behörden nicht ausgenommen.
Das Safe-Harbor-Abkommen ist bekanntlich am 6. Oktober 2015 vom Europäischen Gerichtshof (EuGH, C-362/14) für ungültig erklärt worden, da die USA ein angemessenes Schutzniveau übermittelter personenbezogener Daten nicht gewährleisten. Dies wurde u. a. damit begründet, dass der Zugriff von Behörden, der generell auf den Inhalt elektronischer Kommunikation zielt, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt (siehe auch Beitrag Nummer 3.1).
So ist die derzeitige Orientierungshilfe Cloud-Computing in ihrer Version 2.0 derzeit nun unter Beachtung dieses Urteils anzuwenden und die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA zu unterlassen.

Diese Orientierungshilfe Cloud-Computing 2.0 ist nicht nur in ihrer geänderten Fassung von 2014 anzuwenden, sondern auch unter Beachtung der Entscheidung des Europäischen Gerichtshofes (EuGH) zu Safe Harbor. Die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA ist daher bis auf Weiteres zu unterlassen.

15.10 Newsletter – immer datenschutzgerecht?

Um Informationen an eine bestimmte Zielgruppe regelmäßig oder schnell verteilen zu können, bedient man sich gerne so genannter Newsletter. Newsletter werden in der Regel einmalig versendet. Dennoch ist es nicht unüblich, die versendeten Newsletter für einen späteren Abruf noch einmal auf der entsprechenden Webseite bereitzustellen. Newsletter mit personenbezogenen Daten unterliegen dabei datenschutzrechtlichen Vorschriften. Werden sie nachträglich gespeichert, sind weitere datenschutzrechtliche Vorgaben zu beachten.
Im vorliegenden Fall hatte eine verantwortliche Stelle auf ihrer Webseite die Newsletter gespeichert, um sie für eventuelle Abrufe bereit-

zuhalten. In einem dieser Newsletter waren allerdings auch Fotos von Mitarbeitern und deren Namen veröffentlicht.
Ein ehemaliger Mitarbeiter forderte nun, sein Foto und den Namen aus dem Newsletter von der Webseite zu löschen. Alle Versuche, dies beim ehemaligen Arbeitnehmer durchzusetzen, schlugen jedoch fehl, sodass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hinzugezogen wurde.
Nachdem der TLfDI die Sachlage geprüft und die verantwortliche Stelle kontaktiert hatte, teilte diese mit, alle Fotos des Beschwerdeführers „bei sich“ gelöscht zu haben. Der TLfDI stellte jedoch fest, dass der betroffene Newsletter nach wie vor in der Original-Version abrufbar war. Es stellte sich heraus, dass lediglich alle Links zum Newsletter auf der Webseite gelöscht worden waren. So musste der TLfDI erneut nachhaken und auf Umsetzung drängen. Dem Mangel wurde nun abgeholfen, indem der gesamte Newsletter gelöscht wurde.
Grundsätzlich sind Internetlinks nur Verweise auf Dokumente (wie Webseiten oder eben auch Newsletter), die den Ort und den Namen des Dokumentes im Internet anzeigen. Mit der Löschung des Hinweises auf ein Dokument verschwindet nicht das Dokument selber. Dieses ist unverändert vorhanden. Bei Löschungsbedarf muss also das Original-Dokument gelöscht werden und nicht (nur) alle Verweise darauf.
Die Löschung erfolgte nicht nur aufgrund von „good will“, sondern es bestand tatsächlich eine Verpflichtung hierzu. Eine konkrete Rechtsgrundlage für die Veröffentlichung von Mitarbeiterfotos ist in diesem Zusammenhang nicht ersichtlich. Daher kann die namentliche Veröffentlichung von Mitarbeitern nur mit deren Einwilligung erfolgen (§ 4 Thüringer Datenschutzgesetz).
In der Vergangenheit wurden die Mitarbeiter bei der Aufnahme der Beschäftigung lediglich darauf hingewiesen, dass für den Newsletter und im Rahmen von Veranstaltungen Fotos aufgenommen und ggf. veröffentlicht werden. Soll eine Veröffentlichung im Internet erfolgen, ist das Foto weltweit abrufbar. Eine unberechtigte Weiterverwendung oder Veränderung durch Dritte kann daher nicht generell ausgeschlossen werden. Als Mitarbeiter sollte man daher vorher immer reiflich abwägen, ob man mit der Veröffentlichung von Fotos im Internet einverstanden ist.

Eine Löschung von Links auf abrufbare Dokumente im Internet verursacht noch keine Löschung von Daten in einem Dokument selbst. Nur eine Löschung im Original-Dokument ist hier zielführend. Einwilligungserklärungen müssen zweckgebunden oder besser noch fallbezogen eingeholt werden, sonst sind sie rechtlich unwirksam.

15.11 eIDAS – was ist das?

Mit der Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates der Europäischen Union wurden Regelungen zur elektronischen Signatur für die Mitgliedstaaten getroffen. So regelte nachfolgend das deutsche Signaturgesetz (SigG) die Unterschiede und den Einsatz der elektronischen Signatur, der fortgeschrittenen elektronischen Signatur und der qualifizierten elektronischen Signatur. Einige nationale Normen schreiben zudem die qualifizierte elektronische Signatur vor, wenn die eigenhändige Unterschrift durch eine elektronische Unterschrift im elektronischen Dokument ersetzt werden kann. Um den Bürgern dies zu ermöglichen, sah man auch bereits beim elektronischen Personalausweis einen festen Speicherplatz für die qualifizierte elektronische Signatur vor. So kann man auf dem elektronischen Personalausweis eine qualifizierte elektronische Signatur speichern, um mit dem Personalausweis selbst elektronische Dokumente rechtsverbindlich und fälschungssicher elektronisch zu unterschreiben. Allerdings muss es tatsächlich eine qualifizierte elektronische Signatur sein. Dies bedeutet, ein Zertifizierungsdiensteanbieter hat die Identität des Eigentümers der elektronischen Signatur eindeutig überprüft und dies mittels eines elektronischen Zertifikates belegt. Mithilfe des Zertifikates kann dann festgestellt werden, welcher Person die elektronische Signatur tatsächlich gehört.
Mit der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt vom 8. Juli 2009 wurden alle Mitgliedstaaten zudem verpflichtet, sicherzustellen, dass auch alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch abgewickelt werden können.

Dies bedeutete, auch in anderen Mitgliedstaaten ausgestellte elektronische Signaturen – hierbei insbesondere die qualifizierten elektronische Signaturen – zu prüfen und anzuerkennen.
Da aber europaweit diesbezüglich keine einheitlichen Regelungen vorhanden waren, wurde am 23. Juli 2014 die EU- „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ verabschiedet. Diese Verordnung wird auch als eIDAS-Verordnung bezeichnet (**e**lectronic **id**entification **a**nd trust **s**ervices). Entsprechend dem Erwägungsgrund 3 dieser Verordnung hatte zwar die damalige EU-Richtlinie 1999/93EG Regelungen zu elektronischen Signaturen festgelegt. Dies war jedoch geschehen, ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die eIDAS-Verordnung soll nun die Rechtsvorschrift jener Richtlinie stärken und erweitern.
Diese Verordnung (EU Nr. 910/2014) ist also ein weiterer Baustein, um die Nutzung grenzüberschreitender digitaler Dienste, die sichere elektronische Identifizierung und Authentifizierung und die Förderung des digitalen Binnenmarktes voranzutreiben. Sie gilt mit wenigen Ausnahmen ab dem 1. Juli 2016.
Inhaltlich unterscheidet sich die Verordnung zum Teil vom derzeit noch gültigen Signaturgesetz (SigG). Als Beispiel sei hier die elektronische Fernsignierung genannt: § 5 Abs. 6 i. V. m. § 17 Abs. 1 SigG sieht vor, dass bei der Erzeugung der qualifizierten elektronischen Signatur eine sichere Signaturerstellungseinheit einzusetzen ist und der Antragsteller auch solch eine Einheit besitzen muss. Die EU-Verordnung sieht nun allerdings auch elektronische Fernsignaturen vor, sodass Signaturen beim Vertrauensdiensteanbieter erzeugt und gespeichert werden können (siehe Erwägungsgrund 52, eIDAS-Verordnung).
Die Folgen dieser Regelungen sind aus datenschutzrechtlicher Sicht derzeit noch nicht abzuschätzen. Das hohe Datenschutzniveau in Deutschland hatte bisher sichergestellt, dass für die Signaturerstellung von qualifizierten elektronischen Signaturen bisher nur bei der Bundesnetzagentur gelistete Produkte verwendet werden durften. Mit der nun eingeführten Fernsignatur ist es dem Antragsteller nicht möglich, zu prüfen, ob seine Signatur auch gemäß dem neuesten Stand der Technik erstellt wurde. Es besteht durchaus die Gefahr,

dass der Nutzer nun unwissentlich schlechtere Verfahren auswählt, weil sie preisgünstiger sind.
Interessant für den Nutzer von qualifizierten elektronischen Signaturen könnte auch das „Aussetzen qualifizierter Zertifikate", also das Sperren des oben genannten elektronischen Zertifikates sein. So ist es nun laut eIDAS möglich, bspw. für einen genauen Zeitraum ein qualifiziertes Zertifikat für die qualifizierte elektronische Signatur sperren zu lassen. Aus der qualifizierten elektronischen Signatur wird damit nur noch eine normale elektronische Signatur. Wie oben beschrieben, ist dann eine rechtsverbindliche elektronische Unterschrift nicht möglich, da zu der elektronischen Signatur die dazugehörige Personenüberprüfung mangels gesperrten Zertifikats nicht vorgenommen werden kann.
Denkbar ist so ein solches Szenario bspw. dann, wenn man den Datenträger mit seiner qualifizierten elektronischen Signatur verlegt hat und sicherstellen möchte, dass bis zum Wiederauffinden mit diesem Datenträger kein Missbrauch geschieht, also elektronische Dokumente nicht im eigenen Namen einfach von Dritten unterschrieben werden.
Die EU-Verordnung eIDAS regelt aber nicht nur die Anforderungen an qualifizierte Zertifikate für elektronische Signaturen, elektronische Siegel und für die Website-Authentifizierung, sondern auch Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten.

Durch die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014) wurde für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben. Diese gilt es umzusetzen.

15.12 Kindergartengruppe 2.0 – Unvernunft der Großen zulasten der Kleinen

Eine Kindertagesstätte (Kita) teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass Eltern einer Kitagruppe über einen populären Messengerdienst eine Kontaktgruppe gegründet hätten, innerhalb deren die Erzieherinnen Informationen und Bilder von den Kindern der Kitagruppe verschicken sollten. Bei der App hat man die Möglichkeit, so ge-

nannte Kontaktgruppen einzurichten, zu denen mehrere Gruppenmitglieder gehören können und in denen diese Texte, Bilder und auch Videos austauschen können. Diese Informationen sind allen Mitgliedern der Kontaktgruppe zugänglich und können auch an andere Personen weitergeleitet werden. Laut der Kindertagesstätte lagen im konkreten Fall Einverständniserklärungen der Eltern zur Veröffentlichung von Fotos in Druckmedien und im Internet vor. Es galt nun, vom TLfDI prüfen zu lassen, ob die Einrichtung dieser Nachrichtengruppe datenschutzrechtlich zulässig war und ob die Einverständniserklärungen von den Eltern dafür ausreichend waren.
Die datenschutzrechtliche Prüfung des TLfDI kam zu folgendem Ergebnis:
Für die Anmeldung bei diesem Messengerdienst muss der Nutzer zunächst die Allgemeinen Geschäftsbedingungen (AGB) akzeptieren, die leider nur auf Englisch veröffentlicht sind. In den AGB befindet sich der Hinweis, dass sich der Dienst die nötigen Rechte vorbehalte, Texte, Bilder und andere Inhalte, die ein Nutzer postet, auf weiteren Plattformen und Medienkanälen zu verbreiten. Ferner steht der Dienst immer wieder in der Kritik, das vollständige Adressbuch des Nutzers unverschlüsselt an den US-amerikanischen Server weiterzuleiten.
Der TLfDI wies darauf hin, dass die Kita-Mitarbeiterinnen und -Mitarbeiter weder im Rahmen ihrer Arbeitsverhältnisse noch im Rahmen der bestehenden Verträge zwischen den Eltern und der Kita vertraglich verpflichtet sein dürften, entsprechende Bilder über diese App einzustellen. Demnach dürften die Kita-Mitarbeiterinnen und -Mitarbeiter auch kaum verpflichtet sein, die erwünschten Fotos mit ihren Privat-Smartphones anzufertigen.
Da es sich bei dem Träger der Kindertagesstätte um eine Gemeinde als öffentliche Stelle handelte, hatte somit die Kindertagesstätte als ein Teil einer öffentlichen Stelle auch § 9 des Thüringer Datenschutzgesetzes (ThürDSG) zu beachten. Gemäß § 9 Abs. 2 Satz 1 Nr. 1 ThürDSG haben die von der öffentlichen Stelle zu treffenden technischen und organisatorischen Maßnahmen zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Aufgrund dieser Regelung war nach Prüfung des TLfDI das Übermitteln von Fotos von Kita-Kindern durch Kita-Erzieherinnen in die Kontaktgruppe unzulässig, weil die Kindertagesstätte mit ihren Kita-Mitarbeiterinnen und -Mitarbeitern gerade nicht garantieren konnte, dass die Fotos als personenbezoge-

ne Daten der Kinder von dem Dienst an andere Plattformen und Medienkanäle weitergeleitet werden. Keine Bedenken hegte dagegen der TLfDI, wenn die Kindertagesstätte nicht-personenbezogene Daten – wie z. B. den Hinweis, dass die Kita am folgenden Tag erst eine Stunde später öffnet – in die Kontaktgruppe der Eltern posten würde.

Bedenken bestanden schließlich auch gegen die Übermittlung der Fotos von Kita-Kindern in die Gruppe insoweit, dass aufgrund der oben beschriebenen Weiterleitung der Kontaktdaten an die Firmenserver in die USA auch eine Datenübermittlung in unsicherere Drittstaaten nach § 23 ThürDSG erfolgen könnte, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Der Europäische Gerichtshof (EuGH) hatte in seinem Urteil vom 6. Oktober 2015 die Safe-Harbor-Entscheidung der EU-Kommission, die eine Datenübermittlung unter bestimmten Voraussetzungen in die Vereinigten Staaten von Amerika (USA) gestattete, für unzulässig erklärt. Grund dafür war, dass aus Sicht des EuGH kein angemessenes Schutzniveau für personenbezogene Daten von EU-Bürgern in den USA gewährleistet sei.

Somit wurde der Kindertagesstätte geraten, im Rahmen einer Informationsveranstaltung die Eltern ihrer betroffenen Kitagruppe über die datenschutzrechtlichen Risiken solcher Dienste zu informieren und über andere Möglichkeiten zu diskutieren, wie insbesondere Bilder der Kinder möglichst vielen Eltern auf datenschutzrechtlich sicheren Medien zugänglich gemacht werden können.

Schließlich war noch die Frage zu klären, ob die Kindertagesstätte aufgrund einer Einverständniserklärung der Eltern zur Veröffentlichung von Fotos in den Druckmedien und im Internet datenschutzrechtlich abgesichert ist. Zu beachten war dabei zunächst § 4 Abs. 1 Satz 1 ThürDSG: Danach ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine solche Einwilligung rechtfertigt gemäß § 4 Abs. 1 Satz 2 ThürDSG eine Datenverarbeitung aber nur dann, wenn sie zur Erfüllung anerkannter Zwecke erforderlich ist. Als anerkannte Zwecke im Sinne dieser Vorschrift kommen nach der Begründung zu § 4 Abs. 1 Satz 2 ThürDSG (Drucksache 5/3086) neben der Aufgabenerfüllung öffentlicher Stellen, die vorrangig in den §§ 19 ff. ThürDSG oder spezialgesetzlich geregelt ist, unter anderem behördeninterne Zwecke in Betracht. Somit lag ein anerkannter Zweck im

Fall der Datenerhebung in Form des Einstellens von Fotos der Kita-Kinder durch die Kindertagesstätte in eine Kontaktgruppe aus Sicht des TLfDI nicht vor. Deshalb rechtfertigte schließlich auch eine Einwilligung der Betroffenen hier nicht die Datenerhebung der Kita-Mitarbeiterinnen in Form des Einstellens von Bildern der Kita-Kinder in die Gruppe. Letztlich zu berücksichtigen waren aber auch an dieser Stelle die bereits genannten datenschutzrechtlich unbefriedigenden Zustände in den AGB der App. Aufgrund dessen war es der Kita aus der Sicht des TLfDI unmöglich, die Voraussetzungen des oben genannten § 9 Abs. 2 Nr. 1 ThürDSG zu beachten und einzuhalten, wenn sie Fotos von Kita-Kindern auf die Kontaktgruppe der Eltern einstellen wollte.

Welche Netzwerke bzw. alternativen Dienste dafür infrage kommen, stellt die Seite http://www.youngdata.de/ ausführlich dar (siehe hierzu: www.youngdata.de/whatsapp-skype-co/whatsapp/).

In Messengerdiensten sollten nur personenbezogene Daten eingestellt werden, die auch an Ihrer Haustür hängen oder die Sie auf eine Postkarte schreiben würden. Namen und Bilder von den Kita-Kindern als personenbezogene Daten gehören – gerade wenn beide noch miteinander verknüpft werden (z. B. Bildunterschrift: „Hier sieht man Max Müller und Susi Meyer auf dem Foto.“) – hingegen grundsätzlich nicht in ungeeignete Messengerdienste. Eine öffentliche Kindertagesstätte und ihre Mitarbeiter haben nach § 9 Abs. 2 Satz 1 Nr. 1 ThürDSG die technischen Maßnahmen zu gewährleisten, dass nur befugte Personen personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Da nicht ausgeschlossen ist, dass personenbezogene Daten, die auf diese Weise versandt werden, auch „über den Ozean“ in die USA gelangen und dort von Dritten ungehindert weiterverarbeitet werden, scheidet eine Nutzung von derartigen Diensten in Kindergärten aus. Dies ergibt sich auch aus § 4 Abs. 1 Satz 2 ThürDSG, weil der Einsatz in Kindergärten nicht zur Erfüllung anerkannter Zwecke dient.

15.13 E-Government und Informationstechnik (IT) in der Thüringer Landesverwaltung

Im Mai 2014 veröffentlichte das Thüringer Finanzministerium als zuständiges Ministerium für E-Government eine „Strategie für E-Government und die IT des Freistaates Thüringen“. Dies war entsprechend dem veröffentlichten Dokument notwendig, da zur Bewältigung der vielfältigen Herausforderungen eine Strategie entwickelt werden musste, um langfristig eine gleichgerichtete Vorgehensweise innerhalb der Landesverwaltung und gegenüber den Bürgern und Unternehmen sicherzustellen.
Weiterhin wurde darin verankert, dass die ressortübergreifende Steuerung des E-Governments und der IT in der Landesverwaltung durch den IT-Beauftragten des Freistaats Thüringen (Chief Information Officer – CIO) zu erfolgen hat.
Im August 2015 veröffentlichte das Thüringer Finanzministerium dann eine „Thüringer Organisationsrichtlinie für E-Government“, in der nun die ressortübergreifende Steuerung des E-Governments und der IT in der Landesverwaltung einem im Finanzministerium angesiedelten Beauftragten des Freistaats Thüringen für E-Government und IT übertragen wurde (Thüringer Staatsanzeiger Nr. 37/2015).
Dies erscheint auch für den außenstehenden Betrachter durchaus Sinn zu haben.
War bisher E-Government ein Teilbereich der IT-Strategie, so ist nunmehr ein klares Signal gesetzt worden, dass die IT-Strategie ein Teilbereich ist, um E-Government in der Landesverwaltung durchzusetzen.
Entsprechend dieser Organisationsrichtlinie ist nun eine Koordinierungsstelle E-Government und IT ins Leben gerufen worden, bei der auch der IT-Sicherheitsbeauftragte des Freistaats Thüringen angesiedelt ist. Dessen Aufgabe ist es, den Informationssicherheitsprozess in der Landesverwaltung zu planen, zu koordinieren und zu steuern. Zudem tragen die Zentralabteilungsleiter der Staatskanzlei und der Ministerien als Ressortbeauftragte für E-Government und IT die Verantwortung für E-Government und den IT-Einsatz in ihren Geschäftsbereichen. Sie und der Landesbeauftragte für E-Government und IT bilden den so genannten Lenkungsausschuss E-Government und IT. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat in dem Zusammenhang vorgeschlagen, bei jeweils anstehenden datenschutzrechtlichen Themen

einen Vertreter des TLfDI beratend auch in den Lenkungsausschuss E-Government und IT einzuladen.
Weiterhin gibt es nun den Arbeitskreis „E-Government und IT". Dieser Arbeitskreis setzt sich aus den für IT zuständigen Referatsleitern oder Referenten der Staatskanzlei und der Ministerien, dem IT-Sicherheitsbeauftragten des Freistaates Thüringen und dem Leiter der Koordinierungsstelle E-Government und IT zusammen. Dies ist allerdings nicht neu, denn die für IT zuständigen Referatsleiter der Staatskanzlei und der Ministerien tagten schon immer zusammen, nur der Name des Arbeitskreises änderte sich je nach Zuständigkeiten und Vorgaben.
Egal, wie dieser Arbeitskreis auch benannt ist, stets war und ist der TLfDI in diesem Arbeitskreis als beratendes Mitglied involviert. Dies hat sich aus Sicht des TLfDI auch in all den Jahren bewährt. So müssen nun beispielsweise auch die Konsequenzen des Urteils vom 06. Oktober 2015 vom Europäischen Gerichtshof (EuGH) zur Safe-Harbor-Entscheidung der EU-Kommission bezüglich der Landesverwaltung überdacht werden (siehe dazu Nummer 3.1). Denn das Urteil, welches eine Datenübermittlung von personenbezogenen Daten in die USA auf der Grundlage der Safe-Harbor-Entscheidung für rechtswidrig erklärt, gilt es umzusetzen, auch in einer Landesverwaltung.

Der TLfDI hat vorgeschlagen, ihn bei jeweils anstehenden datenschutzrechtlichen Themen im Thüringer Lenkungsausschuss E-Government und IT beratend hinzuzuziehen. Weiterhin gilt es, das Urteil des Europäischen Gerichtshofs (EuGH) zur Safe-Harbor-Entscheidung der EU-Kommission auch in der Thüringer Landesverwaltung umzusetzen.

15.14 Straßenpanoramafahrten

Neben der Google Inc. und der Microsoft Corporation erfasst nun auch die HERE Global B.V., mit Sitz in den Niederlanden, Panorama- und 3D-Ansichten von Straßenzügen in Deutschland. HERE fertigt 360-Grad-Panoramabilder, 3D-Scans über Laserscanner sowie GPS-Aufzeichnungen an. Damit können 3D-Aufnahmen von Hausfassaden, Vorgärten, Fahrzeugen und anwesenden Personen erstellt werden.

In Thüringen begannen von HERE die Erfassungen von Straßenzügen im Herbst 2014, damals im Auftrag der Firma Nokia. Der TLfDI wies im September 2014 in einer Presseerklärung „Nokia ante Portas“ frühzeitig darauf hin, dass Hausbesitzer (Behörden, Unternehmen, Privatpersonen) in den Panoramabildern ihre Hausfassaden auch gegenüber dieser Firma unkenntlich machen lassen können (https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_zu_nokia_fahrten.pdf).

Die Frage, warum man überhaupt die Straßen befährt und filmt, ist relativ simpel. Es gibt mindestens zwei marktwirtschaftliche Gründe. Zum einen möchte man über Webseiten die virtuelle Darstellung von Straßenzügen so real wie möglich anbieten.
Zum anderen sind die derzeitigen Navigationssysteme in den Autos aus Herstellersicht zu ungenau bzw. nicht nutzerfreundlich genug. Die Idee, beim Autofahren nicht nur den Straßenverlauf einsehen zu können, sondern sich auch an den Fassaden von Gebäuden metergenau orientieren zu können, scheint vor allem von der Automobilindustrie, jedoch auch von den Autofahrern gewünscht. Zudem sollen zukünftig selbstfahrende Autos mit präziseren Navigationssystemen ausgestattet werden. Wie begehrt solche Systeme sind, kann man daran erkennen, dass Presseberichten zufolge die Automobilfirmen Audi, BMW und Daimler im Sommer 2015 den Kartendienst HERE von Nokia für 2,8 Milliarden Euro kauften.
Dem TLfDI ist es wichtig, darauf hinzuweisen, dass, egal welche Firmen gerade solche Straßenpanoramabilder erstellen, ein Widerspruchsrecht zur Veröffentlichung der Aufnahmen besteht. Der TLfDI wird Sie deshalb auch weiterhin auf dem Laufenden halten.

Bei den derzeit gängigen Straßenpanoramafahrten werden in der Regel Bilder vom Straßenverlauf und von Hausfassaden erfasst. Aber auch Vorgärten, derzeitig anwesende Fahrzeuge und Personen könnten dabei zufällig erfasst werden.
Behörden, Unternehmen und Privatpersonen sollten daher die veröffentlichten Daten kritisch betrachten und bei Bedarf ihr Widerspruchsrecht gegenüber der Firma nutzen. Sollte dieses scheitern, wäre der TLfDI über eine Information dankbar.

15.15 YouNow – All know!

YouNow – eine trendige Bühne, um sein Leben mit anderen zu teilen, nicht mal eben mit ein paar hundert Freunden, sondern mit allen Internetnutzern auf dem Globus, jetzt sofort und live. Die Plattform „www.younow.com“ macht es möglich. Vor allem Jugendliche sitzen zu Hause im Kinderzimmer, schalten Handy oder PC-Kamera ein und plaudern mit Chatpartnern. So weit, so alt. Das Besondere an YouNow: Die Internetwelt ist live und ohne Anmeldung dabei. Wer mitplaudern will, kann nach einfacher Anmeldung mit seinem Facebook-, Twitter- oder Google-Account im Chat loslegen oder selbst „broadcasten“ – ganz cool, aber wo ist der Haken?
Vor allem junge Nutzer lassen häufig bewusst oder unbewusst tiefe Einblicke in ihre Privatsphäre zu. Meistens sind sie eindeutig identifizierbar. Es gibt praktisch keine Kontrolle. Das, was vom Nutzer gestreamt und gepostet wird, ist sofort in der Welt. Hinzu kommt: Entsprechend der Datenschutzrichtlinie von YouNow sind jegliche Ersuchen hinsichtlich des Datenschutzes an eine Adresse in New York, USA zu richten. Deutsche, gesetzlich vorgeschriebene Datenschutzstandards sind also kaum durchzusetzen. Zudem haben amerikanische Geheimdienste bei Bedarf den vollen Zugriff auf die Daten.

Der im Jahr 2011 von der YouNow Inc., New York, gegründete Internetdienst (http://www.younow.com/start) gewinnt seit Ende 2014 im deutschsprachigen Raum rasant an Bedeutung. Anlass genug für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), sich mit einem Appell an die Teenager zu wenden, um auf die Besonderheiten dieser Art von Selbstdarstellung im Netz aufmerksam zu machen. Dabei ging es ihm nicht darum, den Zeigefinger zu heben und gar ein „YouNow-Verbot“ zu erteilen. Solche digitale Räume gehören selbstverständlich zu unserer Lebenswelt. Vielmehr sollten beim Streamen einige Regeln beachtet werden, um sich nicht ungewollt selbst in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen. Es geht um ein Stück praktischen Selbstdatenschutz, das ohne viel Aufwand gelebt werden kann.
Die Pressemitteilung des TLfDI vom 20. Februar 2015 (siehe dazu Anlage 53) wurde auch an alle Schulen in Thüringen versandt mit

der Bitte, die YouNow-Problematik im Unterricht aufzugreifen und die praktischen Hinweise in die Klassen zu tragen – auch ein Beitrag des TLfDI zur Medienkompetenzentwicklung der Thüringer Schülerinnen und Schüler. Es bleibt zu hoffen, dass das geschehen ist. Zeitgleich wurde vom TLfDI veranlasst, dass auf dem Thüringer Schulportal ein passendes Video für Jugendliche von einer Mainzer Anwaltskanzlei eingestellt wird. Es wird vom TLfDI für den Einsatz an Thüringer Schulen ausdrücklich empfohlen.

Die Internetplattform YouNow gewinnt seit Ende 2014 im deutschsprachigen Raum rasant an Bedeutung. Sie ermöglicht die Selbstdarstellung in Videostreams und Chats, die unmittelbar von allen Internetnutzern gesehen werden können. Gerade pubertierende Kinder und Jugendliche sollten bei der Nutzung einige Regeln beachten, um sich nicht in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen.
Der TLfDI gab praktische Hinweise zu YouNow an Schulen und forderte zur aktiven Auseinandersetzung im Unterricht auf.

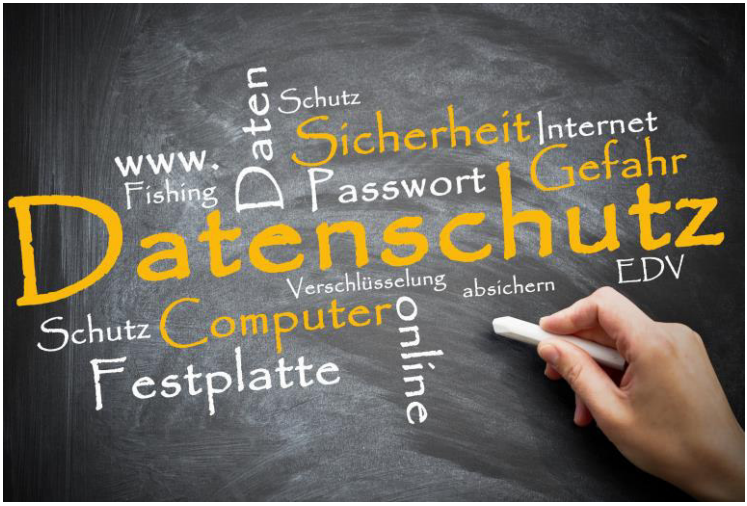
15.16 Daten gelöscht? – Datenschutzgerechte Entsorgung von Hardware

Seit Jahren muss der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) feststellen, dass bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von Festplatten, USB-Sticks und SD-Karten es leider immer noch häufig vorkommt, dass vergessen wird, die darauf befindlichen Daten datenschutzgerecht zu löschen.
Das vollständige Formatieren einer Festplatte oder eines anderen Datenträgers – also die Wiederherstellung des Urzustandes einer Festplatte/eines Speichermediums – ist bspw. zum Löschen ungeeignet, da nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Zuverlässigkeit dieser Löschungsmethode keine Aussage getroffen werden kann (siehe Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02433.html).

Aus diesem Grund informierte der TLfDI erneut im Februar 2015 per Pressemeldung über die datenschutzrechtlichen Möglichkeiten, Daten auf PCs/Laptops und insbesondere auf Smartphones zu löschen (siehe dazu Anlage 52).

Insbesondere erschien es dem TLfDI wichtig, auch die Löschung von Daten auf Smartphones zu problematisieren. Auch hierzu gibt das BSI stets aktuelle Empfehlungen unter:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html.

Bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von Festplatten, USB-Sticks und SD-Karten sind jeweils Löschverfahren nach dem neusten Stand der Technik einzusetzen. Diese werden immer aktuell vom Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Home/home_node.html) veröffentlicht.



Datenschutz – © Marco2811 / Fotolia.com

16 Technische Entwicklung in der Thüringer Landesverwaltung

16.1 Integrierte Teilhabeplanung nun als App

Das damalige Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) hatte in Thüringen die so genannte Integrierte Teilhabeplanung (ITP) eingeführt. Dabei ging es darum, die Ansprüche und Leistungen der Eingliederungshilfe nach § 53 ff. Sozialgesetzbuch (SGB) Zwölftes Buch (XII) für Menschen mit Behinderungen geltend machen zu können. Die Bedarfsermittlung und Hilfeplanung findet im Rahmen des Gesamtplanverfahrens nach § 58 SGB XII statt. Aufgrund der bestehenden fachlichen Anforderungen an ein einheitliches Hilfebedarfsfeststellungsverfahren einigten sich die Kostenträger und die LIGA der freien Wohlfahrtspflege e.V. Ende 2010 darauf, den ITP in Thüringen einzuführen. Gegenstand des ITP ist unter anderem ein Fragebogen zur Ermittlung der Hilfebedarfe von Menschen mit Behinderungen. Die im Fragebogen geforderten Angaben zur materiellen Situation, zu den Vermögenswerten der Hilfeempfänger, zu Familienbeziehungen, Partnerbeziehungen, Beziehungen zu Bekannten oder Freunden, Angaben zur

Religion, Spiritualität und zu Bürgerrechten begegneten aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Bedenken. Nach Aussage des TMSFG waren die geforderten Angaben Inhalt der von der Weltgesundheitsorganisation entwickelten Internationalen Klassifikation der Funktionen (ICF), die Einfluss auf den Hilfebedarf eines Antragstellers sowohl in positiver als auch in negativer Hinsicht haben können. Problematisch war, dass der ITP-Bogen als Grundlage für die Ermittlung von möglichen Teilhabebedarfen ganz verschiedener Zielgruppen dienen sollte und nicht jeder Antragsteller die gleichen Angaben zu machen hatte. Der Bogen sollte vielmehr im Rahmen einer Checkliste entweder gemeinsam mit dem Betreuer oder dem Sachbearbeiter im Sozialamt bearbeitet werden. Der ITP-Bogen sei vielmehr als eine Art Gesprächsleitfaden zu verstehen. Wenn für einen Betroffenen in einem bestimmten Bereich kein Problem und damit auch kein Leistungsanspruch vorlag, musste dieser Bereich auch nicht ausgefüllt und bearbeitet werden. Das barg allerdings Missverständnisse, die eine nicht erforderliche und damit unzulässige Datenerhebung hätten zur Folge haben können. In Abstimmung mit dem TLfDI wurde der ITP überarbeitet. An mehreren Stellen wurde ergänzt, dass bestimmte Angaben nur notwendig sind, wenn sie sich auf die mit dem Sozialarbeiter, mit dem Betroffenen und ggf. seinem Betreuer vereinbarten Ziele zur Integration und ihre Voraussetzungen beziehen. Außerdem wurde vor der Unterschriftszeile nochmals darauf hingewiesen, dass alle gemachten Angaben der Feststellung der Teilhabeleistungen dienen und solche Angaben, die keinen Bezug zu den vereinbarten Zielen haben, nicht erforderlich sind.
Im Anschluss daran wandte sich das TMSFG wiederum an den TLfDI, weil der überarbeitete ITP-Bogen als eigene App im Rahmen des Thüringer Antragsystems für Verwaltungsleistungen (ThAVEL) entwickelt werden sollte. In etlichen Sitzungen mit dem TMSFG und dem für ThAVEL zuständigen Thüringer Finanzministerium (TFM) wurden die Möglichkeiten des Betriebs von ITP als App in dem System ThAVEL beraten. Im Rahmen von ThAVEL wurde im Ergebnis eine neue App entwickelt, die die Bearbeitung des ITP-Bogens auf elektronischem Weg ermöglicht. Hierzu war insbesondere wichtig festzulegen, welche Rollen es im System gibt und welche Rechte diese Rollen jeweils haben. Nicht nur der zuständige Sozialarbeiter sollte Zugriff auf das System haben, sondern eingeschränkt auch bestimmte Leistungserbringer wie Wohnheime oder Werkstät-

ten, in denen die Betroffenen tätig waren. Keinesfalls durfte die App so gestaltet werden, dass jeder jederzeit Zugriff auf alle Daten hat; vielmehr sollten nach dem Grundsatz der Erforderlichkeit die Rechte so vergeben werden, dass immer nur derjenige Zugriff auf die Daten hat, der diese gerade für seine Aufgabenerfüllung benötigt. Die erforderlichen technischen und organisatorischen Maßnahmen wurden in Abstimmung mit dem TLfDI getroffen. Vorgesehen war, dass einige Sozialämter als Modellprojekt die ITP als App prüfen sollten.
Im kommenden Berichtszeitraum wird der TLfDI die Verwendung der ITP-App vor Ort kontrollieren und prüfen, ob die schriftlich festgelegten Zugriffsrechte und sonstigen Berechtigungen in der Praxis so vorgenommen worden sind, wie sie schriftlich im Sicherheitskonzept fixiert wurden.

Der Weg der elektronischen Datenverarbeitung hat in allen Bereichen der Verwaltung Einzug gehalten. Immer mehr Antragsverfahren werden zukünftig elektronisch abgewickelt werden. Dabei ist es sehr wichtig, darauf zu achten, dass alle beteiligten Stellen nur die Zugriffsrechte auf personenbezogene Daten erhalten, die sie tatsächlich für ihre Aufgabenerfüllung benötigen. Es ist ratsam, den TLfDI im Vorfeld bei der Einführung solcher Verfahren zu beteiligen, damit alle datenschutzrechtlichen Anforderungen eingehalten werden.

16.2 Optimierung eines Beihilfe-Kontrollverfahrens oder fragwürdiger Zugriff auf personenbezogene Daten von BALVI iP?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum Kenntnis darüber, dass die Zahlstelle des Thüringer Landesverwaltungsamtes (TLVwA) im Zusammenhang mit Fachkontrollen der zuständigen Veterinärämter einen Abgleich auch personenbezogener Daten von Tierhaltern u. a. zu Kontrollergebnissen und festgestellten Mängeln durchführte, die in der Fachsoftware BALVI iP – diese unterstützt behördliche Kontrollen lebensmittelrechtlicher Vorschriften in überwachungspflichtigen Betrieben – gespeichert würden. Mit diesen Zugriffen bekäme die Zahlstelle des TLVwA möglicherweise auch Kenntnis von personenbezogenen Daten von Tierhaltern, die keine EU-Fördergelder erhielten. Demgegenüber sei den Veterinärämtern bei Einführung von BALVI iP zugesagt worden, dass

keine Zugriffe anderer Behörden auf die Daten der Veterinärämter erfolgen sollte, da allein die zuständigen Fachaufsichtsbehörden, das Thüringer Landesamt für Verbraucherschutz und das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie hierzu befugt seien.
Der TLfDI bat das TLVwA mitzuteilen, zu welchem Zweck die Zahlstelle des TLVwA einen solchen Datenabgleich durchführte und auf welcher Rechtsgrundlage dieses Vorgehen beruhte. Daraufhin teilte das TLVwA dem TLfDI mit, dass es nicht anstrebe, einen Zugriff auf die Fachsoftware BALVI iP zu erhalten. Es würde lediglich versucht, zu analysieren, wie die Vollständigkeit des Kontrollverfahrens zur Vermeidung ungerechtfertigter Agrarbeihilfen sichergestellt werden kann. Die Unvollständigkeit des Kontrollverfahrens beruhe darauf, dass nicht jeder Verstoß gegen die Cross Compliance-Anforderungen – hierbei wird die Zahlung von Agrarbeihilfen von der Einhaltung von Standards des Umwelt-, Lebensmittel-, und Verbraucherschutzes abhängig gemacht – in der Fachsoftware BALVI iP dokumentiert werde.
Abschließend stellte der TLfDI gegenüber dem TLVwA fest, dass es nicht die Aufgabe der Zahlstelle des TLVwA sein könne, die ordnungsgemäße Aufgabenerledigung der Veterinär- und Lebensmittelüberwachungsämter zu überwachen. Diese Beurteilung beruht darauf, dass die Voraussetzungen des § 4 Thüringer Datenschutzgesetz (ThürDSG), wonach die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig ist, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffenen eingewilligt hat, hier nicht vorlagen. Insofern durfte die Zahlstelle des TLVwA nicht zum Zwecke der Überwachung der ordnungsgemäßen Aufgabenerledigung der Veterinär- und Lebensmittelüberwachungsämter auf Daten der Fachsoftware BALVI iP zugreifen.
Da es sich in diesem Falle vorrangig um ein Zuständigkeits- bzw. Organisationsproblem handelte, regte der TLfDI an, in Zusammenarbeit mit Veterinärämtern und ggf. dem TLVwA eine geeignete technisch-organisatorische Lösung zu erarbeiten, die künftig unberechtigte Zahlungen von Agrarbeihilfe auszuschließe, die Verantwortlichkeiten im Kontrollverfahren klar definiere und dabei den gesetzlichen Anforderungen des Datenschutzes und der Datensicherheit Rechnung trage.

Der TLfDI ist auch „Reparaturbetrieb“ für Zuständigkeits-, Organisations- oder Softwareprobleme mit direktem Datenschutzbezug. Seine Aufgabe ist es, in solchen Fällen darüber zu wachen, dass die beteiligten Stellen beim Versuch, die genannten Mängel zu kompensieren, nicht gegen datenschutzrechtliche Bestimmungen verstoßen, und ggf. Empfehlungen zu grundlegenden Lösungsansätzen zu geben.

16.3 Oben ohne – Drohne!

Das Thüringer Innenministerium teilte zur Kleinen Anfrage der Abgeordneten König vom 11. Februar 2014 u. a. mit, dass der Freistaat Thüringen über keine eigenen Drohnen bzw. unbemannte Luftfahrzeugsysteme verfüge und dass die Landesforstverwaltung im Rahmen einzelner operativer Fernerkundungsaufgaben Drohnen von Dienstleistern einsetze (Landtagsdrucksache 5/7689).
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) recherchierte daraufhin, dass ThüringenForst als Anstalt des öffentlichen Rechts Drohnen in verschiedenen Forstämtern zu Testflügen für folgende Zwecke eingesetzt hat:

- zur Kartierung des Borkenkäferbefalls, zur Bilderfassung für das Forsteinrichtungsverfahren, zur Kartierung der Flächenveränderungen nach dem Orkan Kyrill und für Folgemaßnahmen sowie
- zu den Forschungsprojekten Baumartenerkennung, Kronenkartierung, Biodiversitäts-Exploratorien, Kartierung von Baum- und Deichschäden am Leina-Kanal, die durch den Orkan Kyrill verursacht wurden (als Grundlage für ein entsprechendes Planungsverfahren) und zum EU-Forschungsprojekt „BioTree“ zur Dokumentation und Kontrolle von Anwuchs verschiedener Baumarten auf einer forstlichen Versuchsfläche.

Bei diesen Drohnen wurden handelsübliche digitale Kleinbildkameras eingesetzt, jedoch keine Infrarot- und Wärmebildsensoren, die jedoch für bestimmte forstliche Fragestellungen (z. B. Erkennung von Bäumen mit Vitalitätsverlust auf den Color-Infrarot-Bildern im mittleren Infrarot-Kanal oder Wildzählungen mit Thermal-Infrarot-Kameras) geeignet seien.
Programme zur Gesichtserkennung oder WiFi-Sniffer (= Programme zum Auffinden von drahtlosen Rechnernetzen) seien für die Aufga-

ben der Forstverwaltung ohne Interesse und daher weder erprobt noch eingesetzt worden. Nach weiteren Recherchen stellte der TLfDI abschließend fest, dass die von den Flugdrohnen der Landesforstverwaltung gefertigten Aufnahmen keinen Personenbezug aufwiesen. Daher bestanden aus der Sicht des TLfDI in diesem konkreten Fall auch keine datenschutzrechtlichen Bedenken.
Darüber hinaus befragte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum 25 Thüringer Städte mit einer Bevölkerungszahl von über 25.000 Einwohnern danach, ob ihre Stadtverwaltungen derzeit Flugdrohnen nutzten oder ob deren Nutzung vorgesehen sei. Sämtliche angeschriebene Stadtverwaltungen setzten den TLfDI darüber in Kenntnis, dass sie weder Flugdrohnen nutzten noch planten, diese einzusetzen.
Der TLfDI hat am 30. Januar 2015 die Pressemitteilung „TLfDI fordert: Deutschland oben ohne – Drohne!“ veröffentlicht, die auf der Internetseite des TLfDI abrufbar ist (siehe dazu Anlage 51).

Nach den Recherchen des TLfDI steht fest, dass derzeit weder von der Polizei noch von den Landesbehörden oder den Kommunen Drohnen eingesetzt werden, die personenbezogene Daten erheben. Dennoch steht das Thema „Drohneneinsatz“ angesichts des rasanten technischen Fortschritts und der hohen Aussagekraft von Luftaufnahmen unverändert auf der datenschutzrechtlichen Agenda des TLfDI.

16.4 Heimarbeit für Finanzbeamte

Bereits seit Herbst 2008 besteht für den gesamten Außendienst der Steuerverwaltung (Betriebs-, Lohnsteueraußen- und Umsatzsteuersonderprüfer) die Möglichkeit der Inanspruchnahme eines Heimarbeitsplatzes. Voraussetzung für die Genehmigung eines Heimarbeitsplatzes nach der „Rahmendienstvereinbarung zur Einführung von Heimarbeit im Geschäftsbereich des Thüringer Finanzministeriums“ ist neben sicherheitstechnischen Voraussetzungen auch die Einhaltung der datenschutzrechtlichen Vorschriften. Nachdem dies im Jahr 2011 an den Heimarbeitsplätzen von Beauftragten der Finanzämter überprüft worden war, keine Mängel vorlagen und die Einrichtung der Heimarbeitsplätze auch von Seiten der Heimarbeiter sehr positiv angenommen worden war, wurde die Möglichkeit zur

Heimarbeit auf die Kraftfahrttechnischen Beamten und Forstwirtschaftlichen Sachverständigen erweitert. Der eindeutige Vorteil dieser Arbeitsform ist, dass die Beamten weder vor noch nach Erledigung ihrer Aufgaben im Außendienst vor Ort die Dienststelle aufsuchen müssen. Das spart Fahrzeiten und trägt zur Effizienz bei.
Anhand der inhaltlichen Beschreibung der Tätigkeit dieses Beschäftigtenkreises ging der TLfDI davon aus, dass die Dienstposten die typischen Charakteristika der heimarbeitstauglichen Außendiensttätigkeiten in der Finanzverwaltung aufwiesen und hatte keine datenschutzrechtlichen Bedenken, zumal die erforderlichen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben nach § 9 Thüringer Datenschutzgesetz (ThürDSG) getroffen waren. Die wichtigsten Voraussetzungen aus dem datenschutzrechtlichen Blickwinkel sind, dass für unbefugte Dritte keine Möglichkeit der Kenntnis dienstlicher personenbezogener Daten bestehen darf. Das heißt, dass beispielsweise Familienangehörige, Mitbewohner und Besucher des „Heimarbeiters“ keinesfalls Zugang zu dienstlichen Angaben haben dürfen. Hierfür haben zum einen die Dienststelle und andererseits der „Heimarbeiter“ selbst zu sorgen. Hiervon hat sich die Dienststelle regelmäßig zu überzeugen. In der erforderlichen Dienstvereinbarung ist dies konkret auszuführen.
Im Jahr 2015 wurde nun dieses Arbeitsmodell der Heimarbeit auch auf die Dienstposten der Liquiditätsprüfer in den Finanzämtern ausgeweitet werden. Die Tätigkeiten des Beschäftigtenkreises bedingten nicht zwingend eine Erledigung in den Diensträumen der Beschäftigtenbehörden. Unter der Voraussetzung, dass an den Heimarbeitsplätzen die technischen und organisatorischen Maßnahmen zur Gewährleistung der Einhaltung der datenschutzrechtlichen Vorschriften nach § 9 ThürDSG getroffen sind, bestanden auch hiergegen keine Bedenken.

Auch bei Heimarbeit sind wie in der Dienststelle selbst die erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften zu treffen. Insbesondere ist die Möglichkeit der Kenntnisnahme dienstlicher Daten durch unbefugte Dritte auszuschließen.

16.5 Windows XP – baufällig ...

Seit dem 8. April 2014 werden vom Hersteller Microsoft Corporation (Microsoft) für das Betriebssystem Windows XP auch keine Sicherheits-Updates mehr für den erweiterten Support geliefert. Microsoft hatte diesen Fakt bereits Ende 2002 angekündigt und grundlegende Supports schon 2009 eingestellt. Immerhin war das Betriebssystem dreizehn Jahre alt.
Dies birgt für Benutzer, die das Betriebssystem weiterhin benutzen, erhebliche Risiken. Zu vergleichen ist das mit einem alten, maroden Haus, in dem nun die immer wieder eingeworfenen Fensterscheiben nicht mehr mit neuem Sicherheitsglas ausgerüstet werden. Nur so kann ein Glaser (gemeint: der Software-Hersteller Microsoft) dem Zahn der Zeit (gemeint: dem Stand der technischen Entwicklung) trotzen und dem Verfall Einhalt gebieten.
Wo liegen die Probleme?
Aufgrund der fehlenden Sicherheits-Updates durch Microsoft sind personenbezogene Daten auf Windows-XP-Rechnern einem unverantwortlich hohen Risiko möglicher Hacker-Angriffe ausgesetzt.
Nachdem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr, dass trotz der Abkündigung von Windows XP ein Jahr später immer noch Windows-XP-Rechner im Einsatz sein könnten, wandte sich der TLfDI an das Thüringer Innenministerium als kommunale Aufsichtsbehörde mit der Bitte, die Kommunen auf die Risiken beim Einsatz von Windows XP hinzuweisen. Dieses wurde auf wiederholtes Bitten viele Monate später umgesetzt.
Zum anderen wies der TLfDI die obersten Landesbehörden auf die entsprechenden Gefahren hin. Er bat um Rückinformationen, wie viele PCs in den Ressorts noch mit dem alten Betriebssystem arbeiteten. Wenn mit solchen Rechnern noch personenbezogene Daten verarbeitet würden, sollten diese Rechner in der Thüringer Landesverwaltung dringend umgestellt bzw. abgeschaltet werden.
Im Ergebnis teilten die Ministerien für sich und ihre jeweils nachgeordneten Bereiche mit, dass die Windows-XP-Rechner zum Großteil zeitnah abgelöst werden sollen. Allerdings werden – selbst bei Einhaltung der Zeitpläne der Ministerien – nach Redaktionsschluss des vorliegenden Tätigkeitsberichtes ca. 300 Windows-XP-Rechner in der Thüringer Landesverwaltung im Einsatz sein. Davon werden die meisten in Entwicklungs- bzw. Servicebereichen, in der Lehre oder

aber als Messplatz-PCs unter sehr speziellen Einsatzbedingungen verwendet. Hauptgrund dafür ist, dass einige Systeme wegen Software-Unverträglichkeiten (fachenglisch: Inkompatibilität) – insbesondere bei verwendeten älteren Fachverfahren oder aber in medizinischen Geräteumgebungen – nicht mit den neueren Betriebssystemen zusammenarbeiten. Hier müssen Kompromisse geschlossen und Übergangslösungen gefunden werden.
Sollen XP-Rechner weiterhin im Einsatz verbleiben, so ist es notwendig, sie in so genannten abgeschotteten Systemen zu betreiben. Das sind solche Systeme, in denen das Betriebssystem über Browserfunktionen beispielsweise keine aktive Verbindung zum Internet herstellt. Um die Funktionsfähigkeit als abgeschottete Systeme zu gewährleisten, sind explizit technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen zu treffen. Nur so können Sicherheitsrisiken minimiert werden. Eine dieser TOM ist, Einstellungen im Browser oder am Proxy so vorzunehmen, dass der PC keine Internetverbindung aufbauen kann. Aber auch organisatorische Regelungen, wie beispielsweise Dienstanweisungen, zählen zu den TOM. Darin sollte eindeutig vorgeschrieben werden, dass keine Windows-XP-Rechner mehr einen Internetzugang besitzen dürfen und zeitnah ausgetauscht werden sollten. Bei Windows-XP-Rechnern, die wegen spezieller Fachverfahren derzeit immer noch nicht einfach umgestellt werden können, bedarf es zusätzlich einer konkreten Planung mit dem Hersteller dieser Fachverfahren-Software, um die Umstellung der alten auf neuere Software zeitnah zu realisieren.
Mittelfristig bleibt im übertragenen Sinne zum Abriss des alten, maroden Hauses jedoch keine zukunftsorientierte Alternative. Das Betriebssystem Windows XP ist deshalb zeitnah und flächendeckend durch neuere Betriebssysteme zu ersetzen. Dies wurde auch von den obersten Landesbehörden erkannt und eine Umstellung mittelfristig zugesichert.

Das Client-Betriebssystem Windows XP erhält seit April 2014 im erweiterten Support keine Sicherheits-Updates mehr. Es ist daher durch neuere Client-Betriebssysteme zu ersetzen. Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.

16.6 Die Telemedizinplattform Thüringen – ein Blick in die Zukunft der Patientenversorgung

An vielen Stellen werden heutzutage Patientendaten gespeichert: beim Hausarzt, bei Fachärzten, in Krankenhäusern und bei Rehabilitations- oder Pflegeeinrichtungen. Für bestimmte Krankheitsbilder müssen diese verteilten Informationen über den Patienten zusammengeführt werden, um ein korrektes Krankheits- und Therapiebild zu erhalten und eine geeignete Behandlung durchführen zu können. Dies geschieht bisher auf dem klassischen Weg des Arztbriefes, der an andere Beteiligte verschickt wird.
Das Forschungsprojekt „Telemedizinplattform Thüringen“ beschäftigt sich genau mit diesem Aufgabenfeld, nämlich wie dezentral gespeicherte Patientendaten elektronisch über eine einheitliche Oberfläche abgerufen werden können, um so zu einer besseren interdisziplinären Behandlung für zum Beispiel Demenzpatienten zu gelangen. Am Forschungsprojekt sind unter anderem das Universitätsklinikum Jena und die Technische Universität Ilmenau beteiligt.
In der letzten Phase des Forschungsprojektes wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontaktiert und darum gebeten, die vorgestellte Lösung kritisch zu hinterfragen. Kern des Projektes ist eine dezentrale Infrastruktur. Das heißt, hier werden in vielen gleichartig konstruierten Knotenpunkten Patientendaten gesammelt. Ein Knoten könnte ein Krankenhaussystem sein oder das Computersystem einer Pflegeeinrichtung. Ärzte und Hausärzte können über den Webbrowser Daten wie Diagnosen, Medikationspläne und Ähnliches in einem solchen Knoten speichern. In welchem Knoten die Daten gespeichert werden und wer auf diese Daten in welcher Form Zugriff haben darf, wird bei der Konfiguration des jeweiligen Arzt-Zugangs durch das Zugriffs- und Berechtigungskonzept der Telemedizinplattform individuell festgelegt. Zudem sind in keinem Knoten *alle* Patientendaten gespeichert – auch nicht als Kopie. Jeder Knoten funktioniert für sich als Informationsquelle und kann auch lokal genutzt werden, aber er kann von sich aus keine Patientendaten anderer Knoten anzeigen. Um dies sicherzustellen, gibt es zusätzlich ein übergeordnetes Kontrollsystem, welches die Zugriffsrechte netzwerkübergreifend regelt und kontrolliert. Anfragen von einzelnen Knotenpunkten oder den externen Rechnern der Hausärzte werden über die Kontrolleinheit

bewertet und entsprechend den Zugriffsrechten die Dateneinsichten ermöglicht. Der TLfDI bewertete innerhalb des Forschungsprojektes vor allen Dingen die Sicherheitsarchitektur und inwieweit die einzelnen Knotenpunkte als datentragende Stellen gegeneinander vor unrechtmäßiger Kenntnisnahme gesichert waren. Außerdem wurden die Datenflüsse zum Zusammenspiel aller Knotenpunkte und der übergeordneten Kontrolleinheit analysiert sowie die Rechtevergabe für behandelnde Ärzte und das Rechtemanagement untersucht. Im Rahmen des Forschungsprojektes gab es dabei bisher keine Auffälligkeiten. Der TLfDI wird das Forschungsprojekt auch weiterhin begleiten. Allen Beteiligten ist hierbei bewusst, dass das Datenschutzrecht an Forschungsprojekte wesentlich niedrigere Anforderungen stellt als an ein marktreifes Produkt.

Auch bei Forschungsprojekten sind datenschutzrechtliche Anforderungen zu beachten. Bei solchen Neuentwicklungen ist insbesondere „Privacy-by-Design“ gleich zu Beginn zu berücksichtigen. Im vorliegenden Fall wurde dabei auf eine ausreichende Abgrenzung einzelner Teilsysteme geachtet sowie auf das Rollen- und Rechtekonzept und die technischen und organisatorischen Maßnahmen.

update – © Marco2811 / Fotolia.com

17 Vorträge – Der TLfDI ist unterwegs!

Ob Datenschutz in der Schule, bei Gericht, bei Behörden, Hochschulen, Fraktionen oder Parteien, datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Indikatoren sind nicht nur die vielfältigen Eingaben von Bürgerinnen und Bürgern, sondern vor allem auch das gesteigerte Interesse der Medien an datenschutzrechtlichen Themen aller Art. Es vergeht kaum ein Tag, an dem der Schutz der persönlichen Daten nicht in den Nachrichten oder Medien auftaucht. Fast täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herein, ob der TLfDI nicht mit einem „Rund-um-sorglos-Paket“ für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung durch seine Vorträge unterstützen kann. Der TLfDI selbst und einige seiner Mitarbeiter haben im Berichtszeitraum an mehr als **50 (!)** Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im öffentlichen Bereich finden Sie ab Anlage 69.

Nicht verzagen, TLfDI fragen! Der TLfDI freut sich über das gesteigerte Interesse am Schutz der in der Tat bedrohten Privatsphäre und versucht, im Rahmen seiner Möglichkeiten, die Bürgerinnen und Bürger, die Mitarbeiter der Schulen und Unternehmen für das Thema Datenschutz in Thüringen zu sensibilisieren und über den neusten Stand seiner Erkenntnisse zu informieren.

Anlagen

Anlage 1

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.
Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.
Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem

Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.
Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.
Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Anlage 2

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.
Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis “Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).
Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage 3

Anlage zur Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten
   Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographische Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).
2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur
   Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises. Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken

selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung
   Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden. Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten
   Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten
   Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.
6. Ausbau der Angebote und Förderung anonymer Kommunikation
   Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.
7. Angebot für eine Kommunikation über kontrollierte Routen
   Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird. Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden

und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

   Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können. Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

   - alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,
   - für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,
   - eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
   - die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

   Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken. Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen. Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Er-

hebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud-Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik
   Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist. Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung
    Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern. Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik
    Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.
12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit
    Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

Anlage 4

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

„Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke –
Strenge Regeln erforderlich!“

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.
- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.
- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.
- Es ist sicherzustellen, dass
    - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert

und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Anlage 5

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.
Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.
2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-

Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.
4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.
5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.
6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehörd-

licher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

Anlage 6

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

„Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.
Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.
Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass

die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.
An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.
- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Anlage 7

Forderungen
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 28. März 2014 in Hamburg

Unsere Daten sicherer machen - wir selbst haben es in der Hand!

Die bisherigen rechtlichen und politischen Reaktionen auf das massenhafte Ausspähen der Kommunikation durch Nachrichtendienste sind enttäuschend. Das zeigt exemplarisch die Diskussion um das No-Spy-Abkommen.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die am 27. und 28. März 2014 in Hamburg stattfindet, fordert deshalb alle staatlichen und gesellschaftlichen Akteure dazu auf, die Grundrechte der Bürgerinnen und Bürger durch technische und organisatorische Maßnahmen wirksam zu schützen. Die Unversehrtheit der freien und geheimen Kommunikation muss wieder hergestellt werden. Dies erfordert vor allem die Bereitstellung einer von jeder Person einfach nutzbaren Verschlüsselungsinfrastruktur. Sie gilt es insbesondere bei der Kommunikation zwischen Bürger und Verwaltung vorzuhalten. Neben der standardisierten Verschlüsselung beim Transport von Daten muss auch der Einsatz von Mechanismen der Ende-zu-Ende-Verschlüsselung angeboten werden. Außerdem sollten die Angebote zur anonymen Kommunikation sowie die Vertrauenswürdigkeit von Hard- und Software durch Einsatz von Zertifizierungsverfahren ausgebaut werden. Diese Maßnahmen erfordern nicht nur eine Sensibilisierung und Aufklärung der Nutzerinnen und Nutzer durch eine Bildungsoffensive, sondern müssen auch durch eine ausreichende Finanzierung ermöglicht werden.
Hierzu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und amtierender Vorsitzender der Datenschutzkonferenz: „Wir haben es selbst in der Hand, durch die Schaffung einer sicheren IT-Infrastruktur die Hürden für eine massenhafte anlasslose Überwachung unserer Kommunikation durch die Nachrichtendienste wesentlich zu erhöhen. Gerade wenn die politische Kraft nicht ausreicht, den Schutz der Grundrechte auf internationaler Ebene wiederherzustellen, ist die Errichtung technisch organisatorischer Schutzmaßnahmen alternativlos.“

Mit einer Entschließung zur biometrischen Gesichtserkennung durch Internetdienste fordern die Datenschutzbeauftragten zudem, dass die Verarbeitung biometrischer Merkmale der Gesichter der Nutzer in sozialen Medien nur mit der ausdrücklichen und informierten Einwilligung der Betroffenen erfolgen darf. Die individuellen Gesichtsabdrücke der Nutzerinnen und Nutzer werden bei diesen Verfahren dauerhaft und reproduzierbar millionenfach gespeichert. Das Missbrauchspotential derartiger Gesichtsdatenbanken ist immens. Das informationelle Selbstbestimmungsrecht der Betroffenen muss daher bei der Erhebung und Verarbeitung dieser unveränderbaren biometrischen Daten in jedem Fall gewahrt werden.
Die polizeiliche Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke darf künftig nur unter Beachtung strenger Vorgaben erfolgen. Diese Art der Veröffentlichung von Fahndungsdaten greift nicht zuletzt wegen der größeren Reichweite deutlich intensiver in die Grundrechte ein als die herkömmliche Öffentlichkeitsfahndung. Davon sind unter Umständen nicht nur die mutmaßlichen Täter betroffen, sondern auch Zeugen. Die Datenschutzbeauftragten fordern daher unter anderem, dass eine Speicherung der Fahndungsdaten nur auf den Servern der Polizei erfolgen darf. Entscheidend ist zudem, dass die Fahndung nicht als Aufruf zu Hetzjagden und Selbstjustiz im Internet führt. Dazu muss die Kommentierungsfunktion zwingend deaktiviert sein.
Dazu Imke Sommer, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen: „Das letzte Jahr hat uns allen die Augen dafür geöffnet, in welch hohem Maße unser Grundrecht auf informationelle Selbstbestimmung von den großen Datensammlern und allen, die die von ihnen angehäuften Datenberge nutzen, verletzt wird. Wir dürfen jetzt nicht darin nachlassen, alle, die zum Schutz unserer Rechte handeln können, dazu zu bringen, dies auch tatsächlich zu tun.“
Die Datenschutzkonferenz hat die langjährige Forderung zur Schaffung eines nationalen Beschäftigtendatenschutzgesetzes erneut erhoben. Gesetzgeber und Regierung sind aufgefordert, angesichts des Einsatzes mannigfaltiger digitaler Technologien am Arbeitsplatz für einen hinreichenden Datenschutz der Arbeitnehmer und Arbeitnehmerinnen zu sorgen. Die immer stärkere Vermischung von Arbeit und Privatem durch die Nutzung von Handy, Laptop und Dienstwagen mit GPS, aber auch die immer weiter um sich greifende Video-

überwachung am Arbeitsplatz müssen künftig rechtssicher geregelt werden.
Schließlich begrüßt die Datenschutzkonferenz den Entwurf einer Europäischen Datenschutzgrundverordnung, fordert aber in der „Entschließung zur künftigen Struktur der Aufsichtsbehörden in Europa“ Nachbesserungen. Hierbei bekräftigt sie insbesondere den Grundsatz, dass jede Aufsichtsbehörde zur Kontrolle von datenschutzrechtlichen Verstößen befugt ist, wenn Bürgerinnen und Bürger des jeweiligen Mitgliedstaats betroffen sind. Bei grenzüberschreitender Datenverarbeitung soll die Aufsichtsbehörde am Ort der Hauptniederlassung nur federführend tätig werden und eng mit den anderen Aufsichtsbehörden kooperieren. In Streitfällen sollte der Europäische Datenschutzausschuss verbindlich entscheiden.
Andrea Voßhoff, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, unterstreicht: „Eine effiziente Datenschutzaufsicht nahe an den Bürgerinnen und Bürgern muss auch in Zukunft gesichert sein.“

Anlage 8

Entschließungen zwischen den Konferenzen 2014

Keine Vorratsdatenspeicherung in Europa!- Neue Maßstäbe für den Datenschutz
(Umlaufentschließung vom 25. April 2014)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat in einer heutigen Entschließung das Urteil des Europäischen Gerichtshofs (EuGH) zur Europäischen Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) als wegweisend für den Datenschutz in Europa gewürdigt.

Der EuGH erteilt einer anlasslosen und umfassenden Speicherung von Verkehrsdaten eine klare Absage und stützt damit das Recht auf Privatleben und den Datenschutz aller Betroffenen in der EU. Eine undifferenzierte Pflicht zur flächendeckenden Vorratsdatenspeicherung wird sich danach unionsrechtlich nicht mehr begründen lassen. Die Äußerung der Bundesregierung, gegenwärtig keinen nationalen Alleingang zu einer Regelung zur Vorratsdatenspeicherung zu unternehmen, erscheint daher konsequent und ist zu begrüßen.

Dass der EuGH im Übrigen die Pflicht zur umfassenden Verkehrsdatenspeicherung nur für zulässig hält, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen, macht aus Sicht der DSK eine Neubewertung insbesondere der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens erforderlich. Darüber hinaus setzt der Maßstab des EuGH auch der anlasslosen exzessiven Überwachung durch Nachrichtendienste Grenzen.

Dazu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und amtierender Vorsitzender der DSK: „Das Urteil des EuGH festigt die digitalen Grundrechte in Europa gerade zu einer Zeit, in der sie durch Nachrichtendienste systematisch außer Kraft gesetzt werden. Nun gilt es, Konsequenzen aus der Entscheidung zu ziehen. Dabei geht es nicht nur um die Vermeidung undifferenzierter Regelungen zur Vorratsdatenspeiche-

rung. Die EU-Organe wie auch die Mitgliedstaaten sollten darüber hinaus das Urteil zum Anlass nehmen, künftig der massenhaften Vorratsdatenspeicherung durch Nachrichtendienste außerhalb, aber auch innerhalb der EU mit aller Entschiedenheit entgegenzutreten. Nur so wird das Grundrecht auf Datenschutz den Platz einnehmen können, der ihm durch den EuGH gewiesen wurde."

Anlage 9

Entschließung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. Oktober 2014 in Hamburg

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrorda-

teigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief -, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anlage 10

Entschließung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. Oktober 2014 in Hamburg

Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen DoubleClick. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und

den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Anlage 11

Entschließung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. Oktober 2014 in Hamburg

Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen(siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der

Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes – und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit aus reichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.

- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Anlage 12

Entschließung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. Oktober 2014 in Hamburg

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie

auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Anlage 13

Entschließung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. Oktober 2014 in Hamburg

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy-by-design bzw. privacy-by-default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anlage 14

Pressemitteilung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9. Oktober 2014 in Hamburg

Datenschutz erfordert unabhängige Kontrollbehörden

Ob private Unternehmen oder staatliche Stellen – das Recht auf informationelle Selbstbestimmung braucht handlungsmächtige Kontrollinstanzen

Personenbezogene Daten treten immer stärker in den Fokus von öffentlichen und privaten Stellen, die sie in großem Stil erfassen, speichern und verarbeiten. Dabei wird häufig die Sammelwut nur durch die technischen Möglichkeiten begrenzt; ein Ende ist nicht abzusehen. Immer schwerer wird es, der digitalen Technik und der Kapitalisierung von Daten die begrenzende Funktion der Rechte Betroffener entgegenzustellen. Folgerichtig zielen die Forderungen der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum größten Teil auf bessere Kontrollinstrumente und -möglichkeiten durch unabhängige Datenschutzbehörden ab.

Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Einzelnen folgende Entschließungen gefasst:

Effektive Kontrolle der Nachrichtendienste herstellen!
Die Datenschutzkonferenz fordert die Gesetzgeber dazu auf, die Datenschutzbeauftragten des Bundes und der Länder sachgerecht auszustatten. Nur so können sie ihrer Kontrollfunktion, die nicht zuletzt vom Bundesverfassungsgericht im Urteil zum Antiterrordateigesetz unterstrichen wurde, nachkommen. Gleichzeitig gilt es, künftig die Datenschutzbeauftragten bei der Überwachung von Nachrichtendiensten zu beteiligen und ihre Expertise zu nutzen.

Marktmacht und informationelle Selbstbestimmung
Die deutsche Monopolkommission hat für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert. Die Datenschutzkonferenz schließt sich dem an. Zunehmende Unternehmens-

käufe vor allem in der Internetwirtschaft, die wachsende Bedeutung von Big Data sowie die Verflechtung von Internet und Smart Home fordern gemeinsame Strategien.

Unabhängige und effektive Datenschutzaufsicht ist für Grundrechtschutz unabdingbar
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt den Gesetzesentwurf der Bundesregierung, der auf eine Stärkung der Unabhängigkeit der Bundesbeauftragten abzielt. Eine unabhängige Datenschutzaufsicht kann jedoch nur erfolgen, wenn der Behörde ausreichende Personal- und Sachmittel zur Verfügung gestellt werden. Insbesondere muss sich der stetige Aufgabenzuwachs auch in der personellen Ausstattung widerspiegeln. Das gilt auch gerade für viele Datenschutzbehörden in den Ländern, die oft defizitär ausgestattet sind und damit die Grundrechte Betroffener nur unzureichend schützen können.

Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen
Die Datenschutzkonferenz begrüßt die Entscheidung des Europäischen Gerichtshofs zur Löschung von Treffern in der Suchmaschine von Google als „fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet“. Das in dem Urteil geprägte „Recht, schwer gefunden zu werden“ muss nun – der globalen Natur des Internet entsprechend – weltweit umgesetzt werden.

Datenschutz im Kraftfahrzeug
Moderne Kraftfahrzeuge sind längst auch zu umfassenden Datenspeichern geworden. Fahrverhalten, Aufenthaltsorte und Bewegungen des Fahrers oder der Fahrerin können problemlos ausgelesen, zu gänzlich unterschiedlichen Zwecken verwendet und zu Persönlichkeitsprofilen verknüpft werden. Die Datenschutzkonferenz fordert die Automobilindustrie sowie Händler und Werkstätten dazu auf, das Recht auf informationelle Selbstbestimmung auch im Kraftfahrzeug zu gewährleisten.

Dazu Johannes Caspar, der amtierende Vorsitzende der Konferenz: „Datenschutz ist Grundrechtsschutz. Dieser ist in der digitalen Welt immer schwerer zu gewährleisten. Datenschutzbehörden stehen öffentlichen und privaten Stellen gegenüber, die oft auf nahezu uner-

schöpfliche personelle und finanzielle Ressourcen zurückgreifen können. Ein wirksamer Grundrechtsschutz des Einzelnen gegenüber den immer tiefer in das Privatleben eingreifenden Technologien und einer Algorithmisierung unserer Lebenswelt bei der Nutzung digitaler Technologien erfordert gerade auch die Stärkung einer unabhängigen Datenschutzaufsicht in Bund und Ländern sowie eine den wachsenden Herausforderungen angemessene Ausstattung."

Die vollständigen Entschließungstexte der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Ländern sind unter https://www.datenschutz-hamburg.de abrufbar.

Anlage 15

Entschließungen zwischen den Konferenzen 2014/2015

Keine PKW-Maut auf Kosten des Datenschutzes!
(Umlaufentschließung vom 14. November 2014)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-) elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 16

Entschließungen zwischen den Konferenzen 2014/2015

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern (Umlaufentschließung vom 14. November 2014)

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage 17

Entschließungen zwischen den Konferenzen 2014/2015

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern (Anlage zur Umlaufentschließung vom 14. November 2014)

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291 a, 291 b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65 c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalog in Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden.
   Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich.
   Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N-4N)
2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemioloigschen Krebsregist-

rierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. *Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.*

Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jed es für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 04./05. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

Ferner sind hohe (Szenarien 1-2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der

Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI - TR 03116- 1 entnommen sein. (Szenarien 1-4)
5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI - TR 03107-1 zu erfüllen. (Szenarien 1-4)
6. *(optional)* Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291 b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1-4)
7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1-4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsslung einzusetzen. (Szenarien 1-4)
9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)
10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2-4)
11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1-4)

12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein. (Szenarien 1W-4W)
13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2+4)
14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291 a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet. (Szenarien 2W+4W)
15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291 a Abs. 5 c SGB V bestimmt wurden. (Szenarien 2-4)
16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)
17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)
18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19 Ambulante Leistungserbringer müssen die "Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1-4)

20 Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1-4)

21 Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1-4)

22 Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein. (Szenarien 1-4)

23 Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss *(defense in depth).* (Szenarien 1W-4W)

24 Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein

autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W-4W)

25 Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W-4W)

26 Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

27 Da die übermittelten Daten einer folgenden Behandlung zugrundegelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1+4)

28 Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1+4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

29 Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2-4)

30 Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2-4)

31 Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

Anlage 18

Entschließungen zwischen den Konferenzen 2014/2015

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!
(Umlaufentschließung vom 16. Dezember 2014)

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehba-

ren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen

Anlage 19

Entschließung zwischen den Konferenzen 2014/2015

Keine Cookies ohne Einwilligung der Internetnutzer
(Umlaufentschließung vom 5. Februar 2015)

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Artikel 5 Absatz 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sogenannten Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-

Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Anlage 20

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Datenschutz nach „Charlie Hebdo“ :

Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits-und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts –„elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheit-

lich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Anlage 21

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.
- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden

Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich" zu streichen und durch den minder klaren Begriff „eindeutig" zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.
- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.
Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

Anlage 22

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Safe Harbor bietet keinen ausreichenden Schutz
für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

Anlage 23

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist[1]. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

[1] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Anlage 24

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs-und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in

das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o. g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermögliche

Anlage 25

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes,

sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Anlage 26

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfü-

gung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden

   Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Anlage 27

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden ("Predictive Policing").

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien

bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten - in einem Umfang und auf eine Art und Weise - verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

Anlage 28

Gemeinsame Pressemitteilung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 19. März 2015 in Wiesbaden

Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Vor dem Hintergrund der Terroranschläge von Paris weisen die Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 89. Konferenz darauf hin, dass der Datenschutz kein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates ist. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus tatsächlich zielführend und erforderlich sind. Ließe man jeden Eingriff in dieses Grundrecht zu, hätten die Terroristen eines ihrer Ziele erreicht.

Weitere Entschließungen der Konferenz:

Datenschutzgrundverordnung darf keine Mogelpackung werden.

Die Verabschiedung der Datenschutzgrundverordnung geht auf die Zielgerade. Welche Rolle die Bundesregierung in den Verhandlungen spielt, bleibt für die Mitglieder der Datenschutzkonferenz undurchsichtig. Sie warnen eindringlich vor einer Aushöhlung des Datenschutzes. Von wesentlichen Datenschutzgrundsätzen wird durch die jetzt vorgeschlagene Fassung des Kapitels 2 der Datenschutzgrundverordnung abgewichen.
Dies betrifft insbesondere:

- Den Grundsatz der Datensparsamkeit
- Das Zweckbindungsgebot und
- Das Einwilligungsgebot

Zudem wird das Privileg, personenbezogene Daten zu Forschungszwecken zu verarbeiten, über das Recht auf informationelle Selbstbestimmung gestellt.

Damit wird nicht die angestrebte Verbesserung, sondern eine Verschlechterung des Datenschutzniveaus erreicht.

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA.

Der Nachweis, dass amerikanische Sicherheitsbehörden nicht auf personenbezogene Daten zugreifen, die deutsche Unternehmen an US-Unternehmen übermitteln, kann nach den Enthüllungen von Edward Snowden kaum erbracht werden.

Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht unmittelbar anwendbar ist, dürfen damit nach Auffassung der Konferenz nur erfolgen, wenn folgendes sichergestellt ist:

- Einhaltung der Zweckbindung
- Beschränkung staatlicher Zugriffsmöglichkeiten auf ein angemessenes und grundrechtskonformes Maß
- Sicherstellung der Betroffenenrechte (Auskunft, Berichtigung, Löschung)
- Sicherstellung des Rechtsschutzes bei Verstößen.

Verschlüsselung ohne Einschränkungen ermöglichen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Schaffung einer Infrastruktur, die eine verschlüsselte Kommunikation von Bürgern, Verwaltungen, Unternehmen mit- und untereinander ermöglichen. Durch Schaffung einer solchen Infrastruktur kann die Sicherung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet werden. Es ist nach Auffassung der Datenschutzbeauftragten des Bundes und Länder Aufgabe der Politik, dies aktiv zu unterstützen. Eine Einschränkung kryptographischer Verfahren durch staatliche Regulierungen lehnt die Konferenz ab.

Anlage 29

Entschließung zwischen den Konferenzen 2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken
(Umlaufentschließung vom 9. Juni 2015)

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Anlage 30

Entschließung
der 90. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 30. September/1. Oktober 2015 in Darmstadt

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

Anlage 31

Entschließung
der 90. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 30. September/1. Oktober 2015 in Darmstadt

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem "Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes" (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 "Keine Volltextsuche in Dateien der Sicherheitsbehörden" hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbe-

hörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 "Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben"). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 "Effektive Kontrolle von Nachrichtendiensten herstellen!").

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

Anlage 32

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 15./16. September 2015)

Videoüberwachung in öffentlichen Verkehrsmitteln

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit

des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z. B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z. B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw.

dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z. B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwa-

chung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o. Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frageankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maß-

nahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken - wie beispielsweise dem länderübergreifenden Bahnbetrieb - eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z. B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z. B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch

in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z. B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetrieb-

nahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens "Videoüberwachung" mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit

der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträgergespeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art

der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z. B. pauschal eine möglichst umfassende“ Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich z. B. nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter be-

trieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

Anlage 33

Pressemitteilung
vom 31. Januar 2014

Das Auto – Black Box außer Kontrolle

Gestern hat der Verkehrsgerichtstag 2014 klare Regeln für Autodaten gefordert. Eine Forderung, der sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse ausdrücklich anschließt.

Die moderne technische Automobilausstattung bringt es mit sich, dass – zumindest in neueren Fahrzeugen – umfassende Daten über Fahrverhalten und Fahrroute erhoben werden können. Möglich ist sogar, in Erfahrung zu bringen, wann der Fahrer geschaltet und mit welcher Intensität er wo gebremst hat. Bereits jetzt interessieren sich die Kfz-Versicherer für diese Daten und wollen ihre Versicherten dazu bringen, eine Black Box einbauen zu lassen, die das Fahrverhalten ebenfalls beobachtet. Es ist auch nicht auszuschließen, dass derjenige, der in einen Unfall verwickelt ist, in gar nicht ferner Zukunft herangezogen werden wird, seine Fahrzeugdaten zu seiner Belastung auslesen zu lassen – ein Verstoß gegen das im Allgemeinen Persönlichkeits-Grundrecht wurzelnde Selbstbelastungsverbot! Als Gegenleistung soll dann zwar die Versicherungsprämie um etwa 5 % gesenkt werden – bei entsprechend negativem Fahrverhalten wird diese jedoch wieder erhöht werden. Ob hierin noch eine freiwillige Datenpreisgabe des Betroffenen gesehen werden kann, wird derzeit kontrovers diskutiert. Die Gefahren einer derartigen Profilbildung sowie das Wecken von Daten-Begehrlichkeiten liegen auf der Hand.

Virulent wird vor diesem Hintergrund auch die Problematik der Überwachung von Beschäftigten, die z. B. den LKW des Arbeitgebers nutzen.

Das Bundesdatenschutzgesetz hinkt der Realität wieder einmal hinterher. Es legt nicht fest, wem die erhobenen Daten gehören und wer sie zu welchen Zwecken verwenden darf. Oftmals wissen die Fahr-

zeugnutzer nicht einmal, welche Daten über sie erhoben werden und wer diese Daten zu welchen Zwecken nutzt.

„Ich werde mich im Rahmen meiner Möglichkeit dafür einsetzen, dass der Bundesgesetzgeber sich der Thematik annimmt, damit für die Autofahrer in Deutschland die Rechtssicherheit wiederhergestellt wird“, so Dr. Lutz Hasse (TLfDI).

Anlage 34

Pressemitteilung
vom 20. März 2014

§ 28 BDSG – nicht verzagen!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat einen Ratgeber zu § 28 Bundesdatenschutzgesetz (BDSG) erstellt. Bei § 28 BDSG handelt es sich um eine komplizierte, für den juristischen Laien kaum zu verstehende Norm, der jedoch im Datenschutz eine zentrale Bedeutung zukommt.
§ 28 BDSG regelt die Voraussetzungen, unter denen ein Unternehmer zu seinen Geschäftszwecken und Zwecken der Werbung personenbezogene Daten verwenden darf. Nur unter dessen kryptischen Voraussetzungen ist das Verwenden von personenbezogenen Kundendaten zulässig, es sei denn, der Betroffene willigt ein.
Die Broschüre richtet sich ausdrücklich an datenschutzrechtliche Laien und versucht, unverständlichen Gesetzestext für die Unternehmenspraxis zu übersetzen, auch und gerade anhand von Beispielen.

Die Broschüre steht Ihnen auf der Homepage des TLfDI zum freien Download bereit.

Anlage 35

Pressemitteilung
vom 8. April 2014

EuGH kippt Richtlinie zur Vorratsdatenspeicherung –
Hasse: Ein guter Tag, auch für den Thüringer Datenschutz

Die heutige Entscheidung des EuGH zur Vorratsdatenspeicherung bewertet Thüringens Datenschutzbeauftragter Lutz Hasse als „notwendigen Paukenschlag, der die Sammelwut staatlicher Behörden in strikte Grenzen weist. Der EuGH hat dem Datenschutz damit neues Leben eingehaucht, was auch nötig war, nachdem die Enthüllungen von Edward Snowden das Grundrecht der informationellen Selbstbestimmung ins Wanken gebracht hatten."

Das Gericht hatte heute entschieden, dass die EU-Richtlinie 2006/24/EG aus dem Jahr 2006 in vollem Umfang nicht mit der Charta der Grundrechte vereinbar und daher ungültig sei. Daraus folgt für den EuGH, dass die verdachtslose Speicherung von Verbindungsdaten von Telefon, Internet und E-Mails „auf das absolut Notwendige" beschränkt werden müsse.

Der Thüringer Datenschutzbeauftragte begrüßt an der EuGH-Entscheidung vor allem, dass sie den Richtervorbehalt, also die Entscheidung eines Gerichts anmahnt, bevor eine Behörde den Zugang zu den gespeicherten personenbezogenen Daten erhält. Damit werde auch auf europäischer Ebene der Richtervorbehalt zementiert. Ferner zeigt sich Lutz Hasse erfreut darüber, dass die EuGH-Richter auch eine Informationspflicht gegenüber den Inhabern der erhobenen personenbezogenen Daten gefordert haben.

Hasse: „Sowohl den Richtervorbehalt als auch die Pflicht zur Information der betroffenen Bürger habe ich bei der Novellierung des Thüringer Polizeiaufgabengesetzes mehrfach eingefordert und bin damit leider nur zum Teil auf Verständnis gestoßen." Der Datenschutzbeauftragte sieht deshalb in der heutigen Entscheidung auch ein „Signal für den Thüringer Verfassungsgerichtshof", der das Polizeiaufgabengesetz derzeit erneut auf seine mögliche Verfassungswidrigkeit überprüft.

Gleichzeitig mahnt Hasse, nach der EuGH-Entscheidung nicht in „aktionistische Panik“ zu verfallen, sondern die Entscheidungsgründe genau zu studieren. „Schließlich würde es bei der Neufassung des Deutschen Telekommunikationsgesetzes wiederum um einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung gehen“, so Thüringens Datenschutzbeauftragter. „Dessen Verhältnismäßigkeit wäre nicht gegeben, wenn alle Bürgerinnen und Bürger ohne konkret definierten Anlass und weitere differenzierende Kriterien von der Vorratsdatenspeicherung erfasst würden“, so Hasse abschließend.

Die Pressemitteilung des EuGH zur heutigen Entscheidung finden Sie unter:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf

Anlage 36

Pressemitteilung
vom 2. Juni 2014

Arbeitskreis Datenschutz und Bildung
am 2. und 3. Juni 2014 beim Thüringer
Landesbeauftragten für den Datenschutz und die
Informationsfreiheit in Erfurt

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Herr Dr. Lutz Hasse, hat bis auf Weiteres den Vorsitz für den Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Deutschland übernommen.

Erstmals findet nun vom 2. Juni bis zum 3. Juni 2014 der Arbeitskreis Datenschutz und Bildung in den neuen Räumlichkeiten des TLfDI in Erfurt statt.

Schwerpunktthemen sind unter anderem „Young Data“, ein neues Webportal, das viele Antworten für junge Mediennutzer liefert, die Einführung von Medienkunde als eigenes Schulfach sowie die Auswertung des Koalitionsvertrages auf Bundesebene zur digitalen Bildung und zum digitalen Schutz.

Der zweite Sitzungstag beschäftigt sich mit der Überarbeitung des Moduls „Datenschutz“ bei Klicksafe sowie mit den Studien „DIVSI U25“ und „miniKIM“, die das Verhalten der nachwachsenden Generation in Hinblick auf den Medienumgang untersuchen.

Schließlich tauschen sich die Mitglieder über Initiativen in den Ländern aus, um voneinander zu lernen.

Anlage 37

Pressemitteilung
vom 4. Juni 2014

Arbeitskreis Datenschutz und Bildung
in Erfurt richtungsweisend

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Lutz Hasse, tagte der Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 2. und 3. Juni 2014 in Erfurt; in angeregt-konstruktiver Atmosphäre konnten Weichen für die Zukunft gestellt werden:

An der von Jugendlichen stark frequentierten Seite „Young Data“ des rheinland-pfälzischen Datenschutzbeauftragten wollen sich nunmehr mehrere Bundesländer mit eigenen Beiträgen beteiligen; so übernimmt der TLfDI die Themen „Video“ und „Informationsfreiheit“.

Auf große Sympathie stieß die Rede des Herrn Staatssekretärs Prof. Dr. Merten vom Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK). Prof. Dr. Merten maß dem Themenkomplex Medienkompetenz und Datenschutz sowohl an Thüringer Schulen als auch in der Lehrerausbildung große Bedeutung zu. Aufgrund der rasanten Entwicklung der digitalen Medien benötigen die Schulen und Universitäten nach seiner Auffassung nachhaltige Unterstützung, um Schritt halten zu können. Die Kooperation zwischen TMBWK und dem TLfDI solle daher intensiviert werden.

In der Sitzung kristallisierte sich zudem die Bedeutung der frühkindlichen Medienbildung in Vorschulgruppen der Kindertagesstätten heraus. „In diesem Bereich werden die Datenschützer besondere Aktivitäten entfalten“, kündigte Dr. Lutz Hasse an.

Darüber hinaus hat der TLfDI die Aufgabe übernommen, das Modul „Datenschutz“ innerhalb des Internet-Auftritts der EU-Initiative für mehr Sicherheit im Netz „klicksafe.de“ zu überarbeiten und den neuen Entwicklungen anzupassen.

Alles in allem eine weiterführende Veranstaltung; Fortsetzung folgt im Dezember.

Anlage 38

Pressemitteilung
vom 23. Juli 2014

Videogaga: Europäischer Perspektivenwechsel !

Das Problem: Nicht selten videografieren BürgerInnen ihre Mitmenschen auf der Straße oder dem Nachbargrundstück. Das kann beispielsweise mit Kameras im Auto oder in der Brille geschehen. § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) nimmt nun solche Datenerhebungen aus seinem Anwendungsbereich heraus, wenn sie ausschließlich für persönliche oder familiäre Tätigkeiten erfolgen.
Folge: Mangels Anwendbarkeit des BDSG kann der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den aufgenommenen BürgerInnen nicht helfen; diese müssen – auf sich gestellt – beispielsweise das Unterlassen derartiger Aufnahmen vor dem Zivilgericht erstreiten (§§ 823, 1004 BGB).
Neuer Ansatz: In seinem Schlussantrag in der Rechtssache C-212/13 trifft der Generalanwalt am Europäischen Gerichtshofs zu einer auf einem Privatgrundstück fest installierten Videokamera (also – *noch* – nicht zu Handys und Camcordern), die den öffentlichen Raum sowie die Tür eines gegenüberliegenden Hauses erfasst, folgende Feststellungen:
Art. 3 Abs. 2, 2. Spiegelstrich der Europäischen Datenschutzrichtlinie 95/46/EG, der fast wortwörtlich von § 1 Abs. 2 Nr. 3 BDSG als Bundesrecht umgesetzt wird, sei *eng auszulegen*: Zur Beurteilung der Frage, ob die Videoaufnahme ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen werde, komme es *nicht* auf den *subjektiven Zweck* dieser Datenverarbeitung an. Entscheidend sei vielmehr in *objektiver* Hinsicht, ob auch Personen von der Videokamera erfasst würden, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stünden. Für diesen Fall fände die Europäische Datenschutzrichtlinie – und damit ihre engen Zulässigkeitsvoraussetzungen an eine Videoüberwachung - Anwendung.
Schlussfolgerungen für Thüringen: Schließt sich der Europäische Gerichtshof dem Votum des Generalanwalts an, bleibt das BDSG

immer anwendbar, wenn ein Privater Dritte videografiert, die nicht in persönlicher oder familiärer Verbindung zu ihm stehen. Mithin kann der TLfDI dem Betroffenen dann zur Seite stehen und klären, ob nach dem Maßstab des BDSG die Videoaufnahmen rechtswidrig sind. Bejahendenfalls kann der TLfDI geeignete Maßnahmen gegenüber dem Videobetreiber treffen, die die Verletzung des Grundrechts der informationellen Selbstbestimmung unterbinden.
Es würde sich ein weiteres Aufgabenfeld für den TLfDI mit einem effektiveren Grundrechtschutz der BürgerInnen eröffnen – eine gute Entwicklung! ☺

Anlage 39

Pressemitteilung
vom 4. September 2014

EuGH-Urteil: „Recht auf Vergessen“ vs. Archive? – Nein!

Nach dem Urteil des Europäischen Gerichtshofes (EuGH) muss die Internetsuchmaschine Google Einträge in den Suchergebnislisten mit persönlichen Daten auf Verlangen der Betroffenen streichen. Ein Formular zur Beantragung dieser Löschungen hat Google schon kurz nach dem Urteil online gestellt. Nun sind öffentliche Archive besorgt, dieses „Recht auf Vergessen“ gelte auch für sie, sodass möglicherweise auch Archivdaten zu löschen seien. Archive unterliegen indes ganz anderen rechtlichen Rahmenbedingungen als Suchmaschinen. Sie haben u. a. gerade die gesetzliche Aufgabe, Unterlagen, die aufgrund ihres rechtlichen, politischen, wirtschaftlichen, sozialen und kulturellen Wertes als Quellen für die Erforschung und das Verständnis von Geschichte und Gegenwart dienen, dauernd aufzubewahren - § 2 Abs. 2 Thüringer Archivgesetz (ThürArchivG). Zudem setzt der Zugang zu diesen Daten den Nachweis eines berechtigten Interesses sowie die Beachtung schutzwürdiger Belange Dritter voraus, worunter eben auch deren Recht auf Datenschutz fällt (§§ 15 Abs. 7, 16 Abs. 1 und 2 ThürArchivG). Dieser sicheren Datensphäre der Archive stehen Internetsuchmaschinen gegenüber, deren personenbezogene Daten überall auf der Welt mühelos zu vielfältigen Zwecken missbraucht werden können, etwa zur Profilbildung. Allein diese spezifische Internetgefahr wollte der EuGH eindämmen. Daher hat dessen Google-Urteil mangels Vergleichbarkeit keinerlei Auswirkung auf öffentliche Archive.
Es bleibt zu hoffen, dass diese Zusammenhänge bei der Gestaltung der Europäischen Datenschutzgrundverordnung Berücksichtigung finden.

Anlage 40

Pressemitteilung
vom 23. September 2014

Nokia ante Portas

Die in Finnland ansässige Firma Nokia wird nun auch in Thüringen aktiv. Nokia betreibt seit einigen Jahren den Kartierungsdienst „Here“. Die Vermessung wird von der niederländischen Tochter „HERE Europe B.V.“ durchgeführt, die datenschutzrechtliche Verantwortung liegt jedoch weiterhin bei Nokia.

Die Vermessungs-Fahrzeuge sind an dem Schriftzug „here“ und den technischen Kameraaufbauten leicht zu erkennen. Sie fertigen 360 Grad Panoramabilder, 3D-Scans über LIDAR Laserscanner und GPS Aufzeichnungen an. Damit können 3D-Aufnahmen von Hausfassaden, Vorgärten, Fahrzeugen und anwesenden Personen erstellt werden. Wann und wo diese Aufnahmefahrten stattfinden, kann man erfahren unter:

→ http://here.com/legal/driveschedule .

Zufällig aufgenommene Personen, Gesichter oder Autokennzeichen werden laut Nokia in den aufbereiteten Kartendaten unkenntlich gemacht.

Hausbesitzer, die in den Panoramabildern ihre Hausfassade zusätzlich unkenntlich machen möchten, haben die Möglichkeit – auch auf Deutsch – sich per Mail an privacy@here.com oder per Brief an die Nokia Corporation, c/o Privacy, Karakaari 7, 02610 Espoo, Finnland, zu wenden.

Sollten sich weitere Fragen ergeben, finden Sie die Kontaktadresse des zuständigen finnischen Datenschutzbeauftragten unter:
http://www.bfdi.bund.de/SharedDocs/Adressen/EuropaeischeDatenschutzbeauftragte/DatenschutzbeauftragterFinnland.html?nn=409072
Führt dies nicht zum Erfolg, wenden Sie sich bitte an meine Behörde.

Anlage 41

Pressemitteilung
vom 21. Oktober 2014

Datenverschlüsselung geht zur Schule!
Ich mach's mit Safer Mail

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (Thillm) bieten gemeinsam am 23. Oktober 2014 im Erfurter KinderMedienZentrum eine Fortbildung zum Datenschutz an. Sie richtet sich an Pädagogen aller Schularten sowie an Mitarbeiter aus der Schulaufsicht und der Schulverwaltung. Im Mittelpunkt der Veranstaltung „Sicherer Datentransfer durch Verschlüsselung" steht die Ende-zu-Ende-Verschlüsselung von E-Mails. Dies ist ein wichtiges Thema auch für die dienstliche Korrespondenz zwischen Schulleitungen, Schulverwaltung, Lehrern und Eltern, denn oft sind in alltäglichen Nachrichten auch persönliche Daten enthalten, die vor unbefugtem Zugriff zu schützen sind. Nur eine Ende-zu-Ende-Verschlüsselung bietet hier einen sicheren Schutz, der mit vertretbarem Aufwand zu erreichen ist. Das Interesse ist groß, die Anmeldungen überschreiten die mögliche Teilnehmerzahl. Als Hauptreferent konnte Herr Jens Kubieziel gewonnen werden. Der studierte Mathematiker hält Vorträge zur Kryptografie und berät Unternehmen zu IT-Sicherheitsfragen. Die genannte Fortbildung bietet den Teilnehmern breiten Raum für praktisches Ausprobieren der E-Mail-Verschlüsselung und weiterer Sicherheitsmaßnahmen am eigenen Laptop. Deshalb wird in Gruppen von ca. 12 Personen unter kompetenter Anleitung von drei weiteren Fachleuten gearbeitet. Medienvertreter sind herzlich eingeladen, sich vor Ort über den Veranstaltungsverlauf zu informieren. Näheres entnehmen Sie dem Faltblatt.

Anlage 42

Pressemitteilung
vom 17. November 2014

Keine PKW-Maut auf Kosten des Datenschutzes!

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weisen sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die Datenschutzbeauftragten des Bundes und der Länder mahnen die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 43

Pressemitteilung
vom 27. November 2014

„Videogaga als Video“
Kurzfilm zur Videoproblematik als Modul für den Schulunterricht

Alltägliche Erfahrung auf Spielplätzen, Sportanlagen und in Geschäften: Kameras, Kameras, Kameras ... Erfreulich, wenn sich auch Jugendliche fragen – Was soll das denn? Geht das überhaupt in Ordnung? Diese Thematik greift ein Video auf, das vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) konzipiert und von Studenten der TU Ilmenau hergestellt wurde. Gedacht ist es für den Einsatz an den Thüringer Schulen. Dort ist das Thema Datenschutz auch Gegenstand des Kurses Medienkunde in den Klassenstufen 5 bis 10. Der TLfDI verfolgt das Ziel, dass Datenschutz auch wirklichkeitsnah vermittelt werden kann. So Hat seine Behörde ein Unterrichtsmodul für den Einsatz im Unterricht entwickelt, zu dem auch besagter Kurzfilm gehört. Nach Unterrichtserprobung wird das gesamte Modul, bestehend aus Video, Lehrerhandreichung und weiteren Materialien auf der Internetseite des TLfDI und im Thüringer Schulportal downloadfähig sein.
Bis dahin können Neugierige ja schon mal einen Blick in das Video werfen: http://www.tlfdi.de/tlfdi/themen/schule/

Anlage 44

Pressemitteilung
vom 3. Dezember 2014

In's Netz gegangen – Facebook
Fortsetzung: Sachstand & Hinweise

Seit Oktober 2014 ist beim **Bundesverwaltungsgericht** eine Revision in Sachen datenschutzrechtlicher Verantwortlichkeit bei Facebook-Fanpages anhängig.
Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) strebt dabei eine datenschutzrechtlich grundsätzliche Klärung an, inwieweit deutsche Betreiber von Fanpages für die datenschutzwidrige Datenverarbeitung durch den Portalanbieter Facebook mit verantwortlich sind.
In der Pressemitteilung vom 14. Juni 2012 gab der TLfDI bereits einen Überblick über den damaligen Sachstand zum Betreiben von Facebook-Seiten und verwies auf die Entschließung der 82. Konferenz der Datenschutzbeauftragten 2011.
Die Datenschutzbeauftragten des Bundes und der Länder vertraten in dieser Entschließung die Auffassung, dass die öffentlichen Stellen keine Fanpages einrichten sollten.
Dies ist der Tatsache geschuldet, dass von den Besuchern der Fanpages die Nutzungsdaten (IP-Adresse, Informationen durch das Setzen von Cookies, usw.) von Facebook in nicht transparenter Weise erfasst und ohne Einfluss der Betreiber und Besucher der Fanpages verarbeitet werden. Für öffentliche Stellen, die eine Fanpage betreiben, bedeutet dies zudem, dass eine Datenübermittlung an Dritte vorliegt, wofür ggf. die Rechtsgrundlage fehlt. Bis zur endgültigen Entscheidung durch das Bundesverwaltungsgericht sieht der TLfDI das Betreiben von Fanpages weiterhin kritisch und rät daher davon ab.

Anlage 45

Pressemitteilung
vom 11. Dezember 2014

Weihnachtsgeschenk für den Datenschutz!

Etwas verfrühte Weihnachtsbescherung: Heute hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens über die Auslegung von Art. 3 Abs. 2 der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bestätigt, dass auf eine privat betriebene Videoüberwachungsanlage unter bestimmten Voraussetzungen die Europäische Datenschutzrichtlinie und damit das insoweit gleichlautende Bundesdatenschutzgesetz anwendbar ist.

Bereits in der Presseerklärung vom 23. Juli 2014 „Videogaga: Europäischer Perspektivenwechsel" hat der TLfDI auf die Rechtssache C-212/13 beim EuGH und den damit verbundenen Perspektivenwechsel hingewiesen. Gegenstand war eine privat betriebene Videoüberwachungsanlage, die zum Schutz eines Privatgrundstücks auch Teile des öffentlich zugänglichen Raums aufgezeichnet hatte.

Heute hat der EuGH klargestellt: Jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie öffentlich zugänglichen Raum erfasst, fällt in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes; sie ist damit nur unter den dort geregelten Voraussetzungen zulässig.

Der TLfDI freut sich, dass seine bereits seit mehreren Jahren vertretene Rechtsauffassung durch den EuGH bestätigt wurde. Für Thüringen bedeutet dies, dass der TLfDI weiterhin an seiner Kontrollpraxis festhalten und die Rechtmäßigkeit von privat betriebenen Videoüberwachungsanlagen als zuständige Aufsichtsbehörde prüfen wird. Und: Der TLfDI kann damit BürgerInnen, die von solchen Videoaufnahmen betroffen sind, weiterhin unterstützen – ein guter Tag für den Datenschutz und die Privatsphäre! ☺

Anlage 46

Pressemitteilung
vom 19. Dezember 2014

Safe the Date
"Safer Internet Day"
am 10.02.2015
- Medienkunde als eigenes Schulfach -
Neuland in Sicht?

Der Umgang mit modernen Medien ist inzwischen zu einer Grundkompetenz wie Lesen, Schreiben und Rechnen geworden. Unbestritten besteht daher ein bildungspolitischer Auftrag, Kindern und Jugendlichen Medienkompetenz zu vermitteln. In Thüringen und auch in anderen Bundesländern wird der Weg gewählt, die Medienkompetenz im Rahmen des bekannten Schulfächerkanons („integrativ“) zu behandeln. Ob dies das richtige Konzept ist, in Zukunft die Herausforderungen der Mediengesellschaft angemessen zu bewältigen, ist bislang nicht ausreichend hinterfragt worden

Der TLfDI organisiert zu diesem Themenkomplex eine Fachtagung Mit zahlreichen Experten auf diesem Gebiet am

Dienstag, dem 10.02.2015 von 10:00 Uhr bis 17:00 Uhr

im Rathausfestsaal Erfurt, Fischmarkt 1.

Anlage 47

Pressemitteilung
vom 5. Januar 2015

Elektronische Gesundheitskarte ist nun Pflicht!

Seit dem 1. Januar 2015 gilt nunmehr ausschließlich die elektronische Gesundheitskarte (eGK) als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkasse beim Arzt oder Zahnarzt.

Auf der eGK befinden sich alle Daten, die bislang auf der Krankenversichertenkarte enthalten waren sowie zusätzlich das Geschlecht und – außer in den gesetzlich vorgesehenen Ausnahmefällen – ein Lichtbild des Patienten. Hierdurch soll einem Kartenmissbrauch vorgebeugt werden.

Die eGK ist aber darauf ausgerichtet, folgende zusätzliche Funktionen zu erfüllen:

- **Online-Abgleich** der Daten der Karte beim Einlesen in der Praxis mit den bei der Krankenkasse vorliegenden aktuellen Daten des Versicherten; dabei hat die Krankenkasse keinerlei Zugriff auf die beim Arzt vorliegenden Daten;
- Speicherung ärztlicher Verordnungen (sog. **eRezept**) und des Berechtigungsnachweises für EU-Ausländer (sog. **Europäische Krankenversicherungskarte**);
- Zusätzliche Daten können **auf Wunsch des Patienten** gespeichert werden, beispielsweise Notfallversorgungsdaten, ein elektronischer Arztbrief oder persönliche Arzneimittelrisiken und -unverträglichkeiten.

Zunächst soll der Online-Abgleich ab Mitte 2015 in verschiedenen Testregionen erprobt werden, nicht aber in Thüringen. Termine für eine bundesweite Einführung des Online-Abgleichs oder für Tests der weiteren Funktionen stehen noch nicht fest. **Für die Patienten in Thüringen ändert sich also erst einmal nichts.**

Das Projekt wird durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit datenschutzrechtlich begleitet.

Die Kommunikation mit diesen sensiblen Gesundheitsinformationen zwischen Krankenversicherern, Ärzten und Apothekern ist über **ein eigens zu diesem Zweck errichtetes Gesundheitsnetz** vorgesehen, das keine Schnittstelle zum öffentlichen Internet hat. Alle Gesundheitsdaten – auch Rezeptdaten - werden verschlüsselt abgelegt. Sie werden – etwa wenn der Patient dem Arzt oder Apotheker den Zugriff auf diese Daten ermöglichen möchte – durch das gleichzeitige Stecken der eGK und des dem Arzt oder anderen Berechtigten ausgestellten Heilberufsausweises in ein spezielles Kartenlesegerät entschlüsselt.

Darüber hinaus muss der Versicherte einem **Zugriff auf medizinische Daten** durch die Eingabe einer PIN zustimmen. Eine Ausnahme bilden die freiwilligen Notfalldaten, auf die der Heilberufsausweis allein den Zugriff gewährt. Auch für das Entschlüsseln von Rezeptdaten beim Apotheker ist keine PIN erforderlich.

Die Zugriffe auf die eGK werden protokolliert, damit der Versicherte die Zugriffe auf seine Daten einsehen und verfolgen kann.

Mit der vorgesehenen elektronischen Patientenakte wird die eGK voraussichtlich eine weitere Entwicklung erfahren, die der TLfDI beobachten und gegebenenfalls beeinflussen wird.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht für Fragen zur eGK gern zur Verfügung und wird weiter über den Fortgang berichten.

Anlage 48

Pressemitteilung
vom 16. Januar 2015

Non vitae, sed scholae discimus?

„Nicht für das Leben, sondern für die Schule lernen wir“ kritisierte bereits der Philosoph Seneca und mahnte uns zu hinterfragen, ob die Schule junge Leute tatsächlich auf das Leben vorbereitet. Dieses Zitat gewinnt an Würze dadurch, dass sich kürzlich eine 17jährige Schülern mittels Twitter an die Öffentlichkeit wandte und meinte, sie habe mit fast 18 keine Ahnung von Steuern, Miete und Versicherung, könne aber eine Gedichtsanalyse in vier Sprachen schreiben.
Brauchen wir also ein „Unterrichts-Update“?
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) veranstaltet zum internationalen Safer Internet Day am **10. Februar 2015** im Erfurter Rathausfestsaal eine Fachtagung zum Themenkomplex **Medienkunde als eigenes Schulfach**. Besonderes Augenmerk soll dabei auf der Vermittlung von Medienkompetenz liegen. Medienkunde wird in den Schulen bisher ausschließlich integrativ vermittelt, also als Art „Anhängsel“ im Rahmen der bisherigen Schulfächer. Ob die bisherige Stoffvermittlung den gewünschten Erfolg zeigt, welche Defizite hier bestehen und was zu tun ist, soll mit Fachleuten erörtert werden.
Während einer mittäglichen Pressekonferenz wird der Startschuss für das gemeinsame Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes und der Länder (www.youngdata.de) gegeben werden.
Näheres entnehmen Sie bitte dem Flyer.

Anlage 49

Pressemitteilung
vom 28. Januar 2015

Krankenkasse als Fitnesscoach?

Der Presse waren Meldungen zu entnehmen, dass ein großer Versicherer in Europa künftig Fitnessdaten seiner Kunden sammeln will. Als Belohnung für der Gesundheit zuträgliches Verhalten winken dann Gutscheine oder Rabatte auf die zu zahlenden Beiträge zur Krankenversicherung. Die Angebote sollen demnächst auch in Deutschland erhältlich sein.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) befürchtet, dass dies erst der Anfang einer Entwicklung ist, die er sehr kritisch beurteilt. Krankenkassen haben ein zunehmendes Interesse daran, Gesundheitsdaten ihrer Versicherten zu erhalten. Dies aber nicht etwa nur, um sie möglichst effektiv bei der Gesundheitsvorsorge zu unterstützen, sondern zumindest auch, um passgenaue Angebote zu erstellen, damit ihr eigenes finanzielles Risiko so gering wie möglich bleibt.

Der TLfDI warnt: „Sicher ist es verlockend, wegen der Übermittlung von Fitnessdaten ein günstigeres Angebot der Versicherung zu erhalten. Jeder Versicherte sollte sich aber darüber klar sein, dass er seiner Krankenkasse mit diesen Daten sensible Angaben über seine Gesundheit übermittelt. Es ist nicht ausgeschlossen, dass die Krankenkasse anhand dieser Daten auch unliebsame Prognosen über die künftige gesundheitliche Entwicklung treffen kann, die sich für den Betroffenen finanziell ungünstig auswirken können."

Das Problem stellt sich zunächst bei den privat Krankenversicherten. Nach den derzeit für gesetzliche Krankenkassen geltenden Regelungen ist eine Erhebung von Fitnessangaben unzulässig. Auch für die Erhebung im Rahmen einer Einwilligung ist nach Ansicht des TLfDI Dort nach derzeit geltender Rechtslage kein Raum.

Anlage 50

Pressemitteilung
vom 30. Januar 2015

Reminder
"Safer Internet Day" am 10.02.2015
- Medienkunde als eigenes Schulfach -
Neuland in Sicht?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) organisiert eine Fachtagung (s. Faltblatt) mit zahlreichen Experten auf dem Gebiet der Medienkompetenz am

Dienstag, dem 10.02.2015 von 10:00 Uhr bis 17:00 Uhr

im Rathausfestsaal Erfurt, Fischmarkt 1.

Da noch einige Plätze frei sind, werden Interessierte herzlich eingeladen, die Chance zu nutzen und sich anzumelden. Da der Umgang mit modernen Medien inzwischen zu einer Grundkompetenz wie Lesen, Schreiben und Rechnen geworden ist, besteht ein bildungspolitischer Auftrag, Kindern und Jugendlichen Medienkompetenz zu vermitteln. In Thüringen und auch in anderen Bundesländern wird der so genannte „integrative“ Weg gewählt, bei dem die Medienkompetenz im Rahmen des bekannten Schulfächerkanons behandelt wird. Ob dies das richtige Konzept ist, in Zukunft die Herausforderungen der Mediengesellschaft angemessen zu bewältigen, ist bislang nicht ausreichend hinterfragt worden. Der TLfDI freut sich auf eine fruchtbare Diskussion

Anlage 51

Pressemitteilung
vom 30. Januar 2015

TLfDI fordert: Deutschland oben ohne –
Drohne!

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Da können schon Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, den Nacktbadebereich am See oder in sonstige nicht einfach zugängliche Orte.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) weist darauf hin, dass eine legale Drohnennutzung durch **Private** in Deutschland nur unter äußerst engen Voraussetzungen zulässig ist. Zahlreiche Rechtsvorschriften müssen beachtet werden:

Sobald mit der Kamera Menschen gefilmt und damit personenbezogene Daten erhoben werden, müssen das Recht am eigenen Bild und das Grundrecht auf informationelle Selbstbestimmung beachtet werden. Selbst wenn mögliche datenschutzrechtliche Erlaubnisnormen (§§ 6b, 28 und 32 Bundesdatenschutzgesetz) einschlägig wären, würden in aller Regel die schutzwürdigen Interessen der Betroffenen überwiegen. „**Folglich darf mit der Kamera einer Drohne grundsätzlich niemand gegen seinen Willen gefilmt werden**“, betont der TLfDI.

Leider existieren in Deutschland keine verbindlichen eindeutigen Regelungen speziell für Drohnen im zivilen Bereich. Das will die EU jetzt ändern. Sie fordert strenge Regulierung für zivile Drohnen (http://europa.eu/rapid/press-release_IP-14-384_de.htm). Der TLfDI begrüßt diese Entwicklung ausdrücklich. Da die Drohnennutzung in einigen Bereichen, wie im Straßen- und Eisenbahnbrückenbau oder in der Forst- und Landwirtschaft durchaus sinnvoll sein kann, bedarf es konkreter Bestimmungen, wie der datenschutzgerechte Umgang mit Drohnen auszusehen hat.

Einen guten Überblick über die ***luftverkehrsrechtlichen*** Anforderungen gibt die „Kurzinformation über die Nutzung von unbemannten Luftfahrtsystemen“ (unter http://www.bmvi.de//SharedDocs/DE/Publikationen/VerkehrUndMobilitaet/unbemanntluftfahrtsysteme.html).

Anlage 52

Pressemitteilung
vom 6. Februar 2015

Sind sie noch da?

Bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von externen Festplatten, USB-Sticks und SD-Karten kommt es leider häufig vor, dass vergessen wird, die darauf befindlichen Daten datenschutzgerecht zu löschen.

Aus gegebenem Anlass möchte der TLfDI deshalb nochmals darauf hinweisen, dass ein reiner Löschbefehl in der Regel für die Datenlöschung nicht ausreichend ist und somit die Daten mit relativem geringem Aufwand wieder herstellbar sind.

Selbst das vollständige Formatieren einer Festplatte oder eines anderen Datenträgers - also die Wiederherstellung des Urzustandes einer Festplatte/eines Speichermediums - ist zum Löschen ungeeignet, da nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Zuverlässigkeit der Löschung der vorhandenen Daten keine Aussage getroffen werden kann (BSI: Überblick über Methoden zur Löschung und Vernichtung von Daten).

PCs, Laptops:

Auf der Webseite des BSI https://www.bsi-fuer-bueger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen.html finden Sie entsprechende Hinweise zu derzeit vom BSI dem Stand der Technik empfohlenen Lösch-Programme für PCs und Laptops.

Die dort vom BSI empfohlenen Programme zum Überschreiben der Festplatte, die auch zum Teil kostenlos sind, sollten auf jeden Fall Anwendung finden, wenn Sie Ihr Gerät entsorgen oder veräußern möchten. Wichtig ist dabei, dass Sie genau den Anleitungen des Herstellers folgen und die Anleitungen der jeweiligen Lösch-Software genau beachten.

Nachfolgend sollen an Hand des Löschprogrammes DBAN die ersten Schritte erklärt werden, wenn Sie bspw. Daten auf einem Windows XP-Rechner löschen wollen. Wichtig: danach sind alle Daten (inklusive Betriebssystem) unwiderruflich gelöscht:

- Halten Sie eine CD oder einen USB-Stick bereit, worauf Sie das Löschprogramm speichern können.

- Gehen Sie auf die Webseite https://www.bsi-fuer-buer-ger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen.html und informieren Sie sich über die derzeit aktuell empfohlenen Löschprogramme.

- Suchen Sie sich eines der Löschprogramme aus und folgen Sie dem angegebenen Link.

- Beim Lösch-Programm DBAN müssten Sie dann bspw. auf die Webseite von ComputerBild http://www.computerbild.de/download/DBAN-Darik-s-Boot-and-Nuke-945107.html gehen, um die Datei auf einen funktionsfähigen PC herunterzuladen.

- Starten Sie dort „Download“, um die Datei herunter zu laden.

- Diese Datei ist ein ISO-Image und kann nicht von Windows ausgeführt werden, sondern stellt ein eigenes, in sich geschlossenes Betriebssystem dar.

- Sollten Sie über einen CD-Brenner verfügen - brennen Sie diese Datei entsprechend Ihrer Brennersoftware auf die CD.

- Sollten Sie mit einem USB-Stick arbeiten, benötigen Sie noch eine entsprechende Software: (z. B. http://www.computerbild.de/download/ISO-to-USB-6559588.html), um das Lösch-Programm auf den USB-Stick zu „brennen“.

- Wenn der Datenträger entsprechend vorbereitet ist, starten Sie den zu löschenden Rechner, so dass dieser Rechner mit der CD oder dem USB-Stick starten kann.

- Folgen Sie nun den Anweisungen des Programms.

Hinsichtlich der Geräte mit dem Betriebssystem Windows 8 bzw. 8.1, ist auch ein Löschen der Daten direkt möglich. Dies ist allerdings nur der Fall, wenn die Funktion von Windows 8 „Alles entfernen und Windows neu installieren“ und die Option zur gründlichen Löschung gewählt wird. Außerdem muss ebenso sichergestellt sein, dass alle Laufwerke (und nicht nur das Systemlaufwerk) durch die gründliche Löschung erfasst werden, was nur für Laufwerke gilt, die durch Windows lesbar sind. Ist dies nicht möglich, muss wie oben beschrieben verfahren werden.

Smartphones:

Dateien auf Smartphones zu Löschen ist komplizierter. Das Zurücksetzen des internen Speichers auf die Werkseinstellungen bringt meistens keine Datensicherheit.
Wie das tatsächliche Löschen bei Smartphones funktioniert und welches Programm ggf. zum Einsatz kommen sollte, ist für viele Modelle und Betriebssysteme unterschiedlich und bedarf auch hier der korrekten Anwendung der Anleitung des jeweiligen Anbieters. Um die Daten des Smartphones sicher löschen zu können, müssen Sie also die Bedienungsanleitung des Herstellers genau beachten. Einige Hersteller bieten auch auf ihren Online-Portalen spezielle Programme (Apps) zum Löschen an, die das mehrfache Überschreiben mit Zufallsdaten versprechen.

Zudem rät das BSI in seiner Empfehlung „Basisschutz für Smartphone und Co“, auch die SIM-Karte zu entfernen und – falls Sie diese nicht weiter verwenden wollen – zu vernichten.

An dieser Stelle sei nochmal darauf hingewiesen, dass Sie selbst auch zusätzlich die Sicherheit Ihrer Daten auf dem Smartphone erhöhen können:

- Installieren Sie Programme, also Apps, nur von vertrauenswürdigen Quellen.
- Schauen Sie in der Bedienungsanleitung oder im Online-Shop des Herstellers nach, ob Daten auf Ihrem Smartphone verschlüsselt werden können und nutzen sie dies.
- Lassen Sie bei Verlust Ihres Gerätes die SIM-Karte unverzüglich sperren. Manche Hersteller bieten an, dann das Gerät aus der Ferne wenigstens zurückzusetzen oder zu sperren. Ein Zugriff auf die Daten wird dadurch erschwert.

Eins ist sicher – die Frage, ob die Daten auf dem Smartphone noch vorhanden sind, also für Unbefugte wiederherstellbar sind, kann niemand beantworten.

Überlegen Sie sich daher genau, wie Sie Ihren PC, Laptop oder Ihr Smartphone vor der Weitergabe vorbereiten und ob Sie diese Geräte überhaupt in fremde Hände geben wollen.

Auch wenn Sie evtl. dafür momentan sogar einen finanziellen Gewinn erzielen, kann Sie das später teuer zu stehen kommen – Erfahrungswerte aus der täglichen Praxis des TLfDI!!!

Sollten Sie nicht selbst die Daten löschen oder das Gerät nicht physisch zerstören können, sollten Sie eine vertrauenswürdige Computerfirma mit der Löschung der Daten oder Vernichtung des Gerätes beauftragen.

Anlage 53

Pressemitteilung
vom 20. Februar 2015

YouNow – All know!

YouNow – eine trendige Bühne um sein Leben mit anderen zu teilen, nicht mal eben mit ein paar hundert Freunden sondern mit allen Internetnutzern auf dem Globus, jetzt sofort und live. Die Plattform „www.younow.com“ macht es möglich. Vor allem Jugendliche sitzen zu Hause im Kinderzimmer, schalten Handy oder PC-Kamera ein und plaudern mit Chatpartnern. So weit, so alt. Das Besondere an YouNow: Die Internetwelt ist live und ohne Anmeldung dabei. Wer mitplaudern will, kann nach einfacher Anmeldung mit seinem Facebook-, Twitter- oder Google-Account im Chat loslegen oder selbst „broadcasten“. – Ganz cool, aber wo ist der Haken?
Entsprechend der Datenschutzrichtlinie von YouNow sind jegliche Ersuchen hinsichtlich des Datenschutzes an eine Adresse in New York, USA zu richten. Deutsche gesetzlich vorgeschriebene Datenschutzstandards sind also kaum durchzusetzen. Zudem haben amerikanische Geheimdienste bei Bedarf den vollen Zugriff auf die Daten.
Beim Streamen sollten einige Regeln beachtet werden, um sich nicht ungewollt selbst in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen: Seinen Klarnamen, die Wohnadresse, die Schule oder seinen Aufenthaltsort zu bestimmten Zeiten vor der Kamera auszuplaudern, kann sehr gefährlich werden, wenn sich hinter dem scheinbar netten Girl im Chat ein Pädophiler verbirgt, der einen unbedingt persönlich kennenlernen will.
Heimliche Streams aus dem Klassenzimmer mit Mitschülern und Lehrern in Wort und Bild sind zu unterlassen. Nicht nur, weil damit Persönlichkeitsrechte anderer verletzt werden, sondern auch, weil die Aufnahme und Veröffentlichung unbefugt aufgenommener Gespräche nach § 201 StGB unter Strafe steht. Ganz nebenbei: Das Handy, mit dem aufgenommen wurde, wird dabei sehr wahrscheinlich eingezogen werden.
Nicht zuletzt: Wer streamt, sollte keine Musik im Hintergrund laufen lassen, denn die würde ja mit in die Welt geschickt und es ist nicht ausgeschlossen, dass durch die Gesellschaft für musikalische Auf-

führungs- und mechanische Vervielfältigungsrechte (GEMA) Gebühren erhoben werden. Also: **Passt auf Euch auf!**

Anlage 54

Pressemitteilung
vom 15. April 2015

Neuer Beirat beim TLfDI: Frischer Wind!

Nach der Landtagswahl fand am 13.04.2015 die erste und konstituierende Sitzung des Beirats beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) statt. Als neue Vorsitzende wurde die Abgeordnete Katharina König (Die Linke), als Stellvertreter der Abgeordnete Andreas Bühl (CDU) gewählt.

Im Anschluss an die Wahl informierte der TLfDI die Mitglieder über wichtige Projekte seiner Behörde:

Er arbeitet derzeit an Entwürfen zur Novellierung des Thüringer Datenschutzgesetzes und des Thüringer Informationsfreiheitsgesetzes - und darf dabei auch mit der vollen Unterstützung des Beirats rechnen.

Die Länder Berlin, Brandenburg, Thüringen, Sachsen und Sachsen-Anhalt planen, ein Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizei zur Telekommunikationsüberwachung einzurichten. Aufgrund der Eingriffsintensität von solchen Maßnahmen kommt einer intensiven datenschutzrechtlichen Begleitung des Vorhabens ein besonderer Stellenwert zu.

Der TLfDI berichtete außerdem über seine Initiativen im Bereich der Bildung von Medienkompetenz bei Schülern. So wird beispielsweise an einem Thüringer Gymnasium eine vom TLfDI entwickelte Unterrichtseinheit zum Datenschutz mit dem Schwerpunkt „Videoüberwachung“ erprobt. Mit dem Fach/Kurs Medienkunde werden neue Wege zu gehen sein.

Die Mitglieder des Beirates nahmen sich aufgrund dieser zahlreichen aktuellen Datenschutzfragen vor, künftig häufiger als in der letzten Legislaturperiode zusammenzukommen – spannende Zeiten!!! ;-)

Anlage 55

Pressemitteilung
vom 13. Mail 2015

Bei Anruf – Betrug!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse, hat von seinem Berliner Amtskollegen Kenntnis über folgende betrügerische Maschen erhalten, die ihn zu Warnungen veranlasst: Vorgetäuscht wird zu einem der Anruf des Datenschutzbeauftragten oder eines seiner Mitarbeiter, um Kreditkarten- oder Bankdaten zu erfragen. Es wird das Vertrauen zum TLfDI missbraucht und unter dem Deckmantel einer Überprüfung eine vermeintliche Datenpanne vorgetäuscht. Es ist indes abwegig, dass sich der TLfDI mit Bürgern ohne vorherigen schriftlichen Kontakt telefonisch in Verbindung setzt, um sich nach derartigen Daten zu erkundigen. Die erwähnten verdächtigen Anrufe dienen denn auch regelmäßig missbräuchlichen Zwecken. Die Bürger, zumeist ältere Menschen, werden am Telefon aufgefordert, ihre Kartennummern von aufladbaren Kreditkarten – zum Beispiel einer Karte aus dem Supermarkt – zu nennen. Zum Teil werden sie sogar dazu aufgefordert, sich solche Prepaid-Karten im Supermarkt zu besorgen, um dann dem Anrufer – dem vermeintlichen Datenschutzbeauftragten – die Kartennummern zu nennen. Damit hat der Anrufer Zugriff auf das Prepaid-Guthaben. **Bleiben Sie also wachsam!**

Damit nicht genug: Andere Betrüger geben vor, die „Euron Union d.o.o." aus Slowenien zu sein. Sie täuschen nach Überweisung eines dreistelligen Euro-Betrags auf ein Konto den Verkauf eines „EU-Schutzpakets" für private Rufnummern vor, das einen Eintrag in ein „EU-Schutzregister" beinhaltet, um ungewollte Werbung und Anrufe zu minimieren. Auch hierbei handelt es sich um Betrug, denn es kommt zu keinem Eintrag in das Schutzregister.

Der TLfDI warnt davor, persönliche Daten, insbesondere Anschrift und Kontoverbindung, an unseriöse Anrufer oder Adressaten herauszugeben. **Seien Sie vorsichtig!** Gibt es Verdachtsmomente für ein strafbares Verhalten, sollten die Strafverfolgungsbehörden (örtliche

Polizeidienststelle oder Staatsanwaltschaft) informiert werden. Hilfe bieten auch Verbraucherzentralen an – und natürlich der TLfDI :-)

Anlage 56

Pressemitteilung
vom 12. Juni 2015

Datenschutzkonferenz verabschiedet Entschließung gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9. Juni 2015 eine Umlaufentschließung gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten verabschiedet. In ihrer Entschließung weisen die Datenschutzbeauftragten auf ihre erheblichen verfassungsrechtlichen Bedenken gegen den Gesetzentwurf der Bundesregierung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für die Sicherheitsbehörden hin und stellen diesen in Frage. Nachfolgend möchte ich Sie über den Inhalt der Entschließung in Kenntnis setzen:

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015:

Gegen den Gesetzentwurf zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken.

Mit der Vorlage des "Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von TK-Verkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen. Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt. Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde. Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen

unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt. Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird. Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen. Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Anlage 57

Pressemitteilung
vom 3. Juli 2015

Fingerabdruckscanner in der Schule – Finger weg!

- TLfDI nimmt eingesetztes System unter die Lupe -

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist bekannt geworden, dass die Schüler einer Thüringer Grundschule ihr Mittagessen mittels ihrer Fingerabdrücke bestellen und bezahlen können. Der Essensanbieter will dadurch die Bezahlung vereinfachen und effizienter gestalten. Neben der Möglichkeit der Identifizierung des Schülers über den Fingerabdruck besteht dort auch die Möglichkeit der Nutzung eines Funk-Chips. Ob aufgrund der Schaffung dieser Alternativmöglichkeit das Verfahren prinzipiell datenschutzrechtlich zulässig ist, wird der TLfDI zeitnah in der betroffenen Schule datenschutzrechtlich prüfen. Besonderes Augenmerk wird er dabei auf die Datensicherheit der Fingerabdruckdaten und die Verhältnismäßigkeit der Datenverarbeitung legen. Fingerabdrücke sind als biometrisches Merkmal besonders kritisch, da bei einem Datenklau auch die Identität einer Person „kopiert“ werden kann. Dann sind die Folgen über ein ganzes Leben nicht absehbar.

Persönliche Daten, die gar nicht erst erhoben werden, sind am sichersten geschützt!

Unabhängig vom Prüfergebnis rät der TLfDI den betroffenen Eltern von der Nutzung des Fingerabdruckscanners durch ihre Kinder ab, da zudem nicht absehbar ist, welche Begehrlichkeiten die so erhobenen Daten wecken können.

Anlage 58

Pressemitteilung
vom 6. Juli 2015

Schutzbund der Senioren und Vorruheständler Thüringen e.V.

WANTED!
Gesucht werden: Maus-Liebhaber!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) und der Schutzbund der Senioren und Vorruheständler Thüringen e.V. (SBSV) sind gemeinsam auf der Suche nach Menschen für die neue Werkstatt der Generationen. Menschen, die heute in den Ruhestand gehen, haben unter Umständen Jahre ihres Berufslebens am Computer verbracht. Nach Dienstschluss haben sich viele privat weiter mit den spannenden Möglichkeiten der Computertechnik beschäftigt und manche Geheimnisse entdeckt. Sie haben sich komfortable Techniken angeeignet und neue Anwendungen ausprobiert. Dabei sind Schätze an Wissen entstanden. Diese Wissensschätze sollen gemeinsam gehoben und auch anderen zugänglich gemacht werden. Wir suchen Wissende, die ihr Wissen teilen und den Kern einer Initiative bilden wollen, die Silver Surfer und Computerfreaks zusammenbringt. Das Anliegen ist es, gemeinsam zu tüfteln und zu üben, Kenntnisse zu vertiefen und Erfahrungen auszutauschen. Wir wollen mit unserer Kooperation den Erwerb von Medienkompetenz für Seniorinnen und Senioren ermöglichen und Surfer im Netz für den notwendigen Schutz ihrer Daten im Internet sensibilisieren. Der Schutzbund der Senioren und Vorruheständler Thüringen e.V. stellt in seinem Kompetenz und Beratungszentrum am Juri-Gagarin-Ring diese Rahmenbedingungen zur Verfügung. Mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) hat der Schutzbund der Senioren einen engagierten und fachkundigen Partner an seiner Seite. Wer seine Kenntnisse und Fähigkeiten in die **Gründung eines SeniorenComputerClubs (SCC)** in Erfurt einbringen möchte, wendet sich bitte an:
Frau Marianne Schwalbe, Leiterin des Kompetenz- und Beratungszentrums, Juri-Gagarin-Ring 64, in 99084 Erfurt, Tel.: 0361-78929902, E-Mail: schwalbe@seniorenschutzbund.org

Anlage 59

Pressemitteilung
vom 5. August 2015

Windows 10 – Fenster zur Privatsphäre

Seit ein paar Wochen ist das Produkt Windows 10 von Microsoft auf dem Markt. Microsoft bietet sogar ein kostenloses Upgrade, also den Wechsel von alten Windows Betriebssystemen auf Windows 10 an. Zudem wirbt Microsoft damit, dass Windows 10 „voller fantastischer Innovationen" steckt. Richtig! Denn Microsoft hat nun für sich entdeckt, dass Daten über die Nutzer und die verwendeten Geräte und deren Standorte innovativ für Microsoft selbst und für seine Geschäftspartner und Tochterunternehmen genutzt werden können.

Welche Gefahren drohen?

Wie durch die Fachpresse mitgeteilt wird, werden nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten an Microsoft übertragen. Außerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich" angesehen wird (siehe dazu http://www.microsoft.com/de-de/privacystatement/default.aspx, Unterpunkt „Personifizierte Daten, die wir sammeln" – „Mehr erfahren" – „Inhalte")!

Das können Sie tun:

Viele Dienste zur Datensammlung können deaktiviert werden. Dazu müssen Sie bspw. unter dem Punkt „Einstellungen -> Datenschutz" in den 13 Kategorien Ihre persönlichen Einstellungen vornehmen. Eine ausführliche Anleitung, wie man dies bewerkstelligen kann, ist unter http://www.computerbase.de/2015-07/windows-10-test/7/ zu finden.

!Schützen Sie Ihre Daten und Ihre Privatsphäre!

Anlage 60

Pressemitteilung
vom 12. August 2015

Aktenlager in Immelborn - Desaster mit Lerneffekt

Wie noch bekannt sein dürfte, wurden in der kleinen thüringischen Gemeinde Immelborn in einem alten, nicht hinreichend gesicherten Fabrikgebäude hunderttausende Akten unsachgemäß gelagert.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm diesen Vorfall zum Anlass, sich auch mit den dortigen tatsächlichen und rechtlichen Fehlentwicklungen näher zu befassen. Zu diesem Zweck traf er sich regelmäßig mit Unternehmern aus der Aktenarchivierungsbranche und betrieblichen Datenschutzbeauftragten. Gemeinsam entwickelten sie eine **Orientierungshilfe Aktenarchivierung**. Hiermit wird Archivierungsdienstleistern (Auftragnehmern) und Unternehmen / Privatpersonen (Auftraggebern) ein Leitfaden an die Hand gegeben, mit dem sie sich im Dschungel der Vorschriften und deren Auslegungen zurechtfinden sollen. Die Orientierungshilfe unterstützt die Praxis dabei, sich ein Urteil darüber zu bilden, welche Pflichten dem Archivierungsdienstleister obliegen und welche notwendigen Anforderungen der Auftraggeber bei Einlagerung seiner Akten zu beachten hat.

Diese Arbeiten sind nun abgeschlossen. Die Orientierungshilfe legt klar dar, was der Auftraggeber als verantwortliche Stelle bei der Einlagerung, Verwaltung und Vernichtung von Akten zu beachten hat und was ein Archivierungsunternehmen hierfür tatsächlich leisten können muss. Anhand von Checklisten kann ermittelt werden, ob ein Archivierungsunternehmen gemessen an der Brisanz der einzulagernden Akten - z. B. medizinische Akten, Personalunterlagen, geheime Geschäftsunterlagen - für die Auftragserfüllung geeignet ist oder eben nicht. Für Hilfe bei der datenschutzkonformen Vertragsgestaltung sorgen konkrete Hinweise und Muster.

Da die Orientierungshilfe einen bundesweiten Standard zur Verankerung des Datenschutzes in der Archivierungsbranche setzen soll,

wird sie zunächst den Aufsichtsbehörden der anderen Länder zur Abstimmung vorgelegt. Damit möchte der TLfDI erreichen, dass für alle Archivierungsunternehmen in Deutschland einheitliche Anforderungen gelten. Nach diesem Abstimmungsprozess wird der TLfDI die Orientierungshilfe vorstellen.

Anlage 61

Pressemitteilung
vom 18. September 2015

SeniorenComputerClub Erfurt – Start gelungen

Knapp 50 Seniorinnen und Senioren folgten dem Vorschlag, sich zur Gründung von Interessengruppen im SeniorenComputerClub (SCC) beim Schutzbund der Senioren und Vorruheständler Thüringen e. V. im Juri-Gagarin-Ring 56 a zur Auftaktveranstaltung einzufinden. Dieses überwältigende Echo zeigt, dass sich auch Menschen im fortgeschrittenen Alter intensiv mit der digitalen Technik befassen und gern gemeinsam über Neuigkeiten und Probleme diskutieren und zu neuen Erkenntnissen kommen wollen. In Anwesenheit von Dr. Lutz Hasse, dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, stellten Detlef Wagner und Marianne Schwalbe das Konzept des Clubs vor. Innerhalb des Clubs wurden vier Interessengruppen gebildet, die sich mit den Themen: Bild/Film/Musik, Internet, soziale Netzwerke und Windows 10 beschäftigen werden. Eine weitere Gruppe fand sich unter der Bezeichnung „Zum Neustart entschlossen“ zusammen, die sich – wieder – mit dem Thema Computer auseinandersetzen will. Dr. Lutz Hasse stellte in seinem Beitrag die Bedeutung des Internets als Faktor der Lebensqualität mit all seinen Fallen und den erforderlichen Vorsichtsmaßnahmen heraus. Vorträge zu Fragen der Sicherheit im Internet, zu rechtlichen Gesichtspunkten (z. B. Urheberrecht, Bildrechte usw.) und anderen relevanten Aspekten werden in eigens dafür vorgesehenen Veranstaltungen für alle Gruppen angeboten werden. Detlef Wagner, Informatiklehrer und Gründungsmitglied, der sich ehrenamtlich für die Umsetzung der Idee des SCC einsetzt, wird seine Kenntnisse und Erfahrungen in die Gruppen einbringen. „Wir sind auf die Anregungen durch die neuen Gruppen gespannt, erwarten kreative Diskussionen und bieten gern den Rahmen und Unterstützung für diese Form der Weiterbildung“, freut sich Marianne Schwalbe, Leiterin des Kompetenz- und Beratungszentrums.

Anlage 62

Pressemitteilung
vom 6. Oktober 2015

Unsafe harbor

Datenschutzbeauftragter Dr. Hasse: Der EuGH hat den „unsicheren Hafen“ endlich geschlossen

„Mit seinem Urteil zum Safe-Harbor-Abkommen (zu Deutsch: Sicherer-Hafen-Abkommen) hat der Europäische Gerichtshof (EuGH) die Rechtspositionen der Datenschutzbeauftragten des Bundes und der Länder deutlich gestärkt – dies ist ein Meilenstein für den Datenschutz in Europa, Deutschland und in Thüringen“, kommentiert Thüringens Datenschutzbeauftragter, Dr. Lutz Hasse, die Entscheidung der Luxemburger Richter. Der EuGH habe den „unsicheren Hafen“, so Hasse, heute zu Recht geschlossen und dessen Regelungen für ungültig erklärt, weil sie keinen ausreichenden Schutz vor Grundrechtseingriffen durch amerikanische Behörden geboten hätten. „Das haben die deutschen Datenschutzbehörden seit den Enthüllungen Edward Snowdens im Sommer 2013 immer wieder kritisiert“, erinnert Lutz Hasse. Seine KollegInnen und er hatten seit damals die Aussetzung einer Datenübermittlung in die USA, basierend auf dem Safe-Harbor-Abkommen, gefordert, weil dessen Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und der Zweckbindung eines behördlichen Datenzugriffs von US-amerikanischen und anderen Sicherheitsdiensten schlichtweg ignoriert wurden. Erfreut zeigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch über den klaren Hinweis des EuGH, dass die Kommission keine Kompetenz hatte, die Befugnisse der nationalen Datenschutzbehörden mit der Unterzeichnung des Safe-Harbor-Abkommens zu beschränken. Hasse: „Damit stärken die Luxemburger Richter erneut die Unabhängigkeit der Datenschutzbehörden.“ Zudem empfahl Hasse, die geplanten Regelungen der neuen EU-Datenschutz-Grundverordnung im Lichte dieser sehr deutlichen EuGH-Rechtsprechung zu überdenken. „Man muss sich nun die Zeit nehmen, die Auswirkungen dieses wegweisenden Urteils auf die vorgesehene Datenschutz-Grundverordnung

zu erkennen und deren Regelungen an der Entscheidung ausrichten“, so der TLfDI.

Anlage 63

Pressemitteilung
vom 3. November 2015

Kein Wildwuchs mehr bei Videoüberwachung im ÖPNV

Videoüberwachung nimmt in allen Lebensbereichen zu. Diese Entwicklung hat leider auch vor Zügen, Straßenbahnen und Bussen nicht halt gemacht. Trotz oder gerade weil in diesem Segment das Instrument der Videoüberwachung sehr geschätzt ist, wird sie oft über das zulässige Maß hinaus eingesetzt. Der Kameraeinsatz muss da enden, wo das Bundesdatenschutzgesetz die Grenzen für diese Art der Datenerhebung setzt. Zu diesem Zweck haben die Aufsichtsbehörden der Länder unter wesentlicher Beteiligung von Mitarbeitern des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine neue Orientierungshilfe für den Bereich Videoüberwachung in öffentlichen Verkehrsmitteln erarbeitet. Darin wird eine aktuelle, umfassende und klare Position der Aufsichtsbehörden für den Datenschutz zum Einsatz von Videotechnik in öffentlichen Verkehrsmitteln zum Ausdruck gebracht. Die Orientierungshilfe finden Sie auf unserer Homepage zum Download. (https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_v_____pnv_stand_09_2015_dk.pdf)

Eine Videoüberwachung ist eine Datenerhebung, die, wie in allen anderen Bereichen auch, im Einklang mit dem Grundrecht auf informationelle Selbstbestimmung der Fahrgäste stehen muss. So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können einen besonders intensiven Eingriff dar, der in aller Regel nicht zulässig sein dürfte. Entscheidend sind aber immer die besonderen Umstände des Einzelfalles. Daher wendet sich das Papier an Unternehmer, um Hilfestellung zu leisten, eine Videoüberwachung im Einzelfall gesetzeskonform auszurichten. Auch ausschreibenden Institutionen gibt sie eine notwendige Orientierung. Denn bei den derzeitigen Ausschreibungen für Busse und Bahnen sehen sich Unternehmer oftmals außer Stande, eine gesetzeskonforme Videoüberwachung zu installieren, die den gesetzlichen Vorgaben entspricht.

Anlage 64

Pressemitteilung
vom 20. November 2015

NEU: Digitale Selbstverteidigung –
Youngdata hat die Tipps für Kids

Kindern und Jugendlichen stehen heute zahlreiche Möglichkeiten der Mediennutzung offen. In den meisten Fällen sind sie jedoch noch nicht in der Lage, die Vorteile und die Gefahren, die sich daraus ergeben, richtig einzuschätzen und danach zu handeln. Datenschutz als Schutz der Privatsphäre spielt dabei eine ganz wesentliche Rolle. Seit zwei Jahren gibt es ein Internet-Angebot der Datenschutzbeauftragten des Bundes und der Länder – Youngdata – ein seit dem Safer Internet Day 2015 gemeinsames Portal, das sich mit Datenschutzinformationen gezielt an Kinder und Jugendliche richtet. Hier finden die Kids Informationen zum Datenschutz und zur Informationsfreiheit, Tipps für ein kluges Verhalten im Internet und Berichte über die digitale Zukunft unserer Gesellschaft. Youngdata enthält Informationen zum Selbstdatenschutz bei der Nutzung von Facebook, WhatsApp, Skype & Co., YouTube, Spielekonsolen, Smartphones und anderen Anwendungen. Es klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen. Zum zweijährigen Bestehen wird diese Internetseite jetzt um eine Rubrik erweitert – die „Digitale Selbstverteidigung“. Diese leider erforderlich gewordene Rubrik gibt Tipps, die helfen sollen, private Informationen zu schützen. Sie zeigt auf, welche Möglichkeiten junge User haben, durch ihr eigenes Verhalten digitale Spuren zu vermeiden und die Kontrolle über ihre Daten zu behalten. Die Pflege der Rubriken von Youngdata erfolgt im Wege einer Arbeitsteilung bei den einzelnen Landesdatenschutzbeauftragten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat als Vorsitzender des Arbeitskreises Datenschutz und Bildung den Bereich „Informationsfreiheit“ und „Videoüberwachung“ übernommen.

Anlage 65

Pressemitteilung
vom 1. Dezember 2015

Revolution
beim 13. Arbeitskreis Datenschutz und Bildung
Wow – das ging ab:

Vom 30. November bis zum 1. Dezember tagte der 13. Arbeitskreis (AK) Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Erfurt unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Lutz Hasse. In dieser Funktion hatte der TLfDI in Berlin Kontakt zu der Ständigen Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kurzform: Kultusministerkonferenz, Abk. KMK) aufgenommen. Vertreter der KMK waren heute erstmals im AK anwesend – und: Sie haben intensiv eine Kooperation zwischen der KMK und den Datenschutzbeauftragten der Länder, speziell mit dem AK Datenschutz und Bildung angefragt. „Das ist revolutionär!“, so Dr. Lutz Hasse gemeinsam mit den Vertretern der KMK. Die Datenschutzbeauftragten wollen sich zusammen mit den zuständigen Gremien der KMK u. a. der drängenden Frage widmen, wie Medienkompetenz Schülern, Studenten, Lehrern und auch Eltern in attraktiver Weise nahe gebracht werden kann. Der AK Datenschutz und Bildung hatte in den letzten Jahren stets bemängelt, dass es auf diesem Gebiet nicht voran ging, obwohl die Defizite offenkundig waren. Nun aber soll es endlich losgehen; euphorisiert werden die Datenschützer versuchen, diesen Prozess möglichst zu beschleunigen. Mit von der Partie ist auch unsere Kultus-Staatssekretärin Frau Gabi Ohler, die – speziell mit Blick auf Thüringen – den Datenschutz (inklusive TLfDI) bzw. den Schutz der Privatsphäre bei der Vermittlung von Medienkompetenz umfassender einbinden will. Hasse: „War wirklich sehr angetan von der heutigen Aufbruchsstimmung und hoffe, dass wir aus dem heutigen und den künftigen Meilensteinen einen frostsicheren Medienkompetenz-Weg bauen können, für Schüler, Lehrer und Eltern!“

Anlage 66

Pressemitteilung
vom 2. Dezember 2015

Premiere: Heilmittel für Krankenhäuser
TLfDI startet speziellen Blog zu Datenschutzproblemen im Gesundheitsbereich

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Herr Dr. Lutz Hasse lädt Sie zum offiziellen Start des TLfDI-Blogs für Krankenhäuser auf seiner Internetstartseite www.tlfdi.de ein.

Wann: Mittwoch, 9. Dezember 2015, 10 Uhr
Wo: Behörde des TLfDI, Häßlerstraße 8, 3. Etage, 99096 Erfurt

Bei dem Blog des TLfDI ist ein geschlossener Bereich für Krankenhäuser eingerichtet. Dieser ist nur für erfolgreich registrierte und freigegebene Benutzer, sprich Thüringer Krankenhäuser, die sich über die Landeskrankenhausgesellschaft autorisiert haben, zugänglich. Es ist eine Plattform, auf der sich Krankenhäuser anonym mit ihren Fragen zum Datenschutz an den TLfDI wenden können. Weitere Blogs sind in der Pipeline.

Ziel ist es, dass Krankenhäuser, die erfahrungsgemäß eine Fülle von Datenschutzproblemen zu bewältigen haben, ihre Fragen anonym an den TLfDI richten können, damit derartige Probleme nicht "hinter dem Berg" gehalten werden. Nur so können wir die bisweilen komplexen Schwierigkeiten erkennen, sezieren und Wege zur Genesung anbieten.

Anlage 67

Pressemitteilung
vom 9. Dezember 2015

TLfDI startet als erster Landesdatenschützer ein Internet-Forum für Krankenhäuser!

Erfurt, 9. Dezember 2015: Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse und der Geschäftsführer der Landeskrankenhausgesellschaft Thüringen e. V. (LKHG), Michael Lorenz starteten heute mit einem offiziellen Knopfdruck das erste Internet-Forum für Krankenhäuser auf der Website eines Landesdatenschutzbeauftragten. Es handelt sich dabei um ein geschlossenes Forum, das nur für erfolgreich registrierte und freigegebene Thüringer Krankenhäuser, zugänglich ist. Die Krankenhäuser haben sich zuvor über die LKHG autorisiert. „Die Landeskrankenhausgesellschaft Thüringen e. V. unterstützt die Einrichtung dieses Forums. Die Thüringer Krankenhäuser können sich nunmehr bei datenschutzrechtlichen Fragestellungen schnell und unkompliziert an den Landesdatenschutzbeauftragten Thüringens wenden“, so Michael Lorenz. Ziel ist es, dass Krankenhäuser, die täglich mit einer Fülle von Datenschutzproblemen konfrontiert werden, ihre Fragen **anonym** an den TLfDI stellen können. „Nur so werden die bisweilen komplexen Schwierigkeiten offen angesprochen und gemeinsam auf einen guten Weg zur Heilung gebracht“, sagte Hasse. Beim Pressetermin wurde mit einer Live-Vorführung demonstriert, wie der Ablauf von der Anmeldung bis zur Antwort funktioniert. Hasse: „Ich empfange Signale, dass Krankenhäuser auf dieses Forum warten – gut; unser Angebot ist gemacht.“

Anlage 68

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres

29.Oktober 2015
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 9. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DSGVO) im Paket zum Jahresende 2015.
Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012[2] mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August 2015 hat sie zu den Trilogverhandlungen zur DSGVO Stellung genommen[3]. Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben[4]. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“ und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im Anwendungsbereich der JI-Richtlinie hingewiesen.

[2] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6
[3] Trilogpapier der Konferenz zur DSGVO, abrufbar unter: https://www.datenschutz.hessen.de/entschliessungen.htm
[4] Stellungnahmen zur DSGVO und zur JI-Richtlinie vom 11.6.2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012, jeweils abrufbar unter
https://www.datenschutz.hessen.de/entschliessungen.htm und
https://www.datenschutz.hessen.de/taetigkeitsberichte.htm

Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert[5].

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI-Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht

[5] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.
Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.
Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DSGVO. Denn die DSGVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit“ erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DSGVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die JI-Richtlinie Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter

einem Rechtsakt – der JI-Richtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DSGVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DSGVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DSGVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf“. Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der

Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden[6].
Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar" mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).
Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff")[7].

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

[6] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 5.
[7] BVerfGE 100, 313, 389; ständige Rechtsprechung.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtiger Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert.
Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records“, Art. 23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten" der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen) Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Demgegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltschaftlichen Verfahrensakten die Regelung, dass die Ausübung der

Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht“ erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt des Art. 17 JI-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der JI-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 JI-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwaltschaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung - Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 JI-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie“. Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar“ sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik“ („state of the art“) sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der JI-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare“ Technik bzw. Technologie sollte konsequenter Weise

auch in der JI-Richtlinie durch „Stand der Technik“ ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25a (2) lit. b erwähnten „biometrischen Daten“ gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinienvorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der Definition der „biometrischen Daten“, wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art.

35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in internationalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentationspflicht gemäß Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV ver-

langen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die JI-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Anlage 69

4. Konferenz für Lehrer, Erzieher und
Sonderpädagogische Fachkräfte
14. April 2014

beim THÜRINGER MINISTERIUM FÜR BILDUNG,
WISSENSCHAFT UND KULTUR (TMBWK)

Inhalt:
Überblick zum Datenschutzrecht
- Datenschutz ist Grundrecht!
- Datenschutzrecht in Thüringen
- Datenschutzbestimmungen im Schulbereich

Ausgewählte Aspekte zum Datenschutz in der Schule
- Veröffentlichungen der Schule
- Kommunikation Schule – Lehrer – Schüler – Eltern

Anlage 70

Veranstaltung im Staatlichen Gymnasium Neuhaus/Rwg
15. April 2015

Inhalt:
Das Grundrecht auf informationelle Selbstbestimmung
Rechtliche Grundlagen für den Datenschutz in der Schule

Anlage 71

"Datenschutz in der verwaltungsgerichtlichen Justiz"
Thüringer Verwaltungsrichterverein
19. Juni 2014

Datenschutz in der Justiz

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (**TLfDI**)

Inhalt:

Anlage 72

2. Tandemfortbildungsveranstaltung für Schulsozialarbeiterinnen und Schulleitungsmitglieder“
Thematik: Erfolgreiches Agieren im Rahmen des gesetzlichen Datenschutzes, 26. Juni 2014

und

Jahrestagung: "Schulbezogene Jungendsozialarbeit - das erste Jahr"
15. Juli 2014
Organisationsberatungsinstitut Thüringen - ORBIT –

Inhalt:
TLfDI
Rechtliche Grundlagen
Warum Datenschutz?
Datenschutz in der Schule
Datenschutz in der Schulsozialarbeit
Einzelfälle

Anlage 73

HWK Erfurt Veranstaltung,
12. November 2014

Wie kann ich vorsorgen

Datenschutz im Internet

Dipl.–Ing. Jens Keßler

Mitarbeiter Referat 3
Technischer und organisatorischer Datenschutz beim

Thüringer Landesbeauftragten für den Datenschutz und die
Informationsfreiheit (TLfDI)

Inhalt:

Anlage 74

Gewerkschaft Erziehung und Wissenschaft
Landesverband Thüringen (GEW)
13. November 2014

Novelle des Thüringer Personalvertretungsgesetzes Umsetzung der Änderungen in § 68 ThürPersVG - Wahrung des Datenschutzes für alle Beschäftigten

Inhalt:
Der TLfDI!
Was ist Datenschutz?
Datenschutz im Rechtssystem
Thüringer Datenschutzgesetz und die Arbeit des Personalrates

Anlage 75

Datenschutz für Personalratsmitglieder
THÜRINGER MINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND KULTUR (TMBWK)
14. November 2014

Inhalt:
Der TLfDI!
Was ist Datenschutz?
Datenschutz im Rechtssystem
Thüringer Datenschutzgesetz und die Arbeit des Personalrates
Speziell: Datenschutz im Schulbereich und Einzelfälle

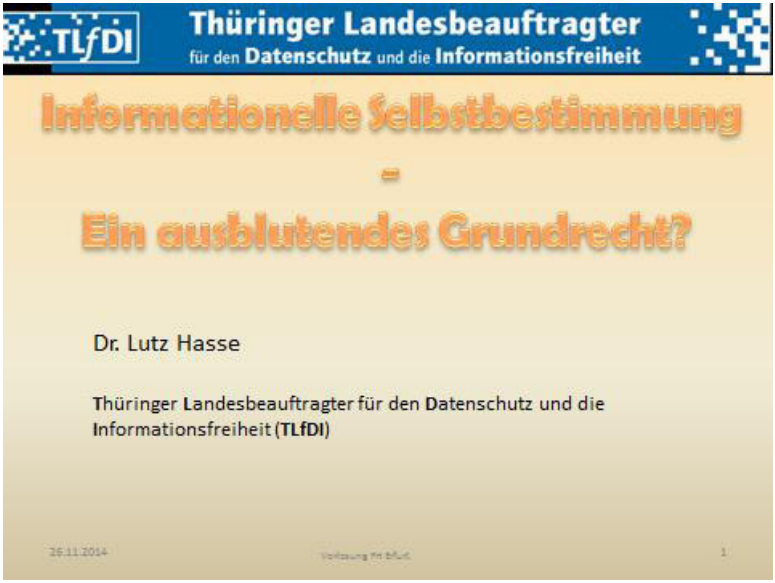
Anlage 76

Datenschutz im Schulbereich und Einzelfälle
Datenschutz in der Erwachsenenbildung
Landesorganisation der freien Träger in der Erwachsenenbildung e. V., LOFT
21. November 2014

Inhalt:
Der TLfDI!
Was ist Datenschutz?
Datenschutz im Rechtssystem
Welche Regelungen gelten für Bildungseinrichtungen nach BDSG?
Welche Daten darf ich erheben?
Fallstricke bei der Teilnehmerwerbung

Anlage 77

Konsequenz bei Verstößen,
Regelungen im ThürDSG
Fachhochschule Erfurt,
26. November 2014



Inhalt:
Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

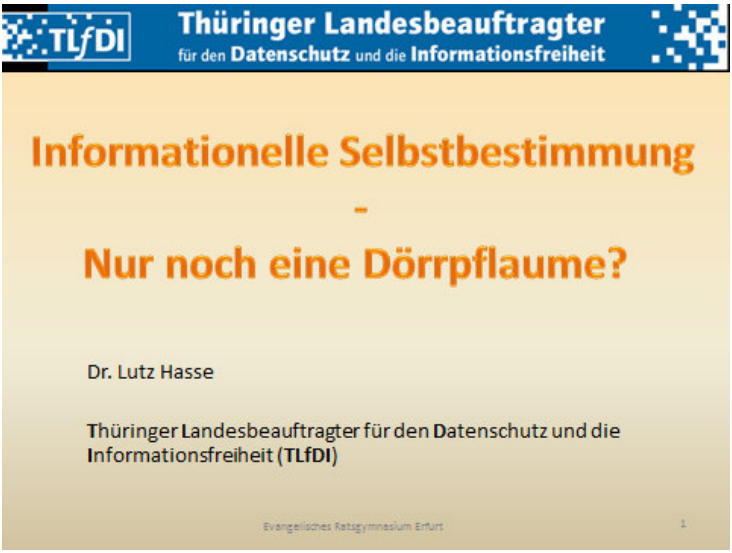
Anlage 78

Veranstaltung der Fakultät für Mathematik und Informatik
der FSU Jena
7. Januar 2015

Inhalt:
Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

Anlage 79

Evangelisches Ratsgymnasium in Erfurt
25. Februar 2015



Inhalt:

Art. 6 Abs. 2 Verfassung des Freistaats Thüringen
Definition personenbezogene Daten – § 3 BDSG/ThürDSG
Art. 6 Abs. 3 Verfassung des Freistaats Thüringen
Verbot mit Erlaubnisvorbehalt – § 4 Abs. 1 BDSG/ThürDSG
Datenverarbeitung
Rechtsgrundlagen
Rechtliche Grundlagen für den Datenschutz in der Schule
Thüringer Schulgesetz
Thüringer Schulordnung
Veröffentlichungen von Stunden- und Vertretungsplänen
Veröffentlichungen im Internet
Soziale Netzwerke

Anlage 80

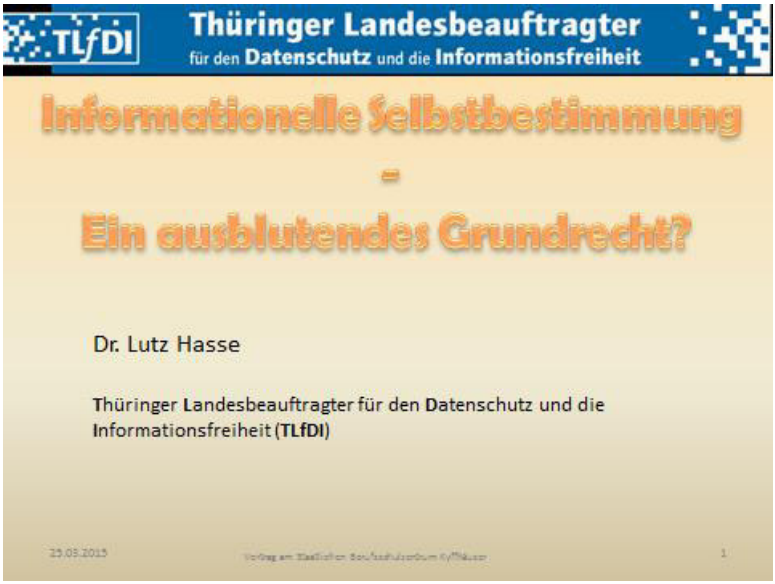
1. Datenschutztag Karl-Volkmar-Stoy-Schule Jena
2. März 2015

Inhalt:

Motivation:
Was ist das Internet?
Was wird im Internet genutzt?
Was kann passieren?
Verschlüsselung:
Gegenmaßnahmen
GPG im Detail
HTTPS

Anlage 81

Vortrag am Staatlichen Berufsschulzentrum Kyffhäuser
25. März 2015



Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

Anlage 82

Fraktionsveranstaltung,
Bündnis 90/Die Grünen
13. Mai 2015

Inhalt:

Was ist überhaupt „E-Health“?
Vorteile und Gefahren
Rechtsgrundlagen
Aktuelle Beispiele und News
Europa

Anlage 83

FSU Jena – Institut für Politikwissenschaft
25. Juni 2015

Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?

Anlage 84

„Grundkenntnisse im Datenschutzrecht“
Thüringer Volkshochschulverband e.V.
24. Juni 2015

Grundkenntnisse im Datenschutzrecht

Saskia Springer
Referentin bei im
Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI)

1

Inhalt:
Die Behörde des TLfDI!
Historischer Hintergrund zum Datenschutzrecht
Verfassungsrechtliche Grundlagen
Datenschutzrechtliche Grundsätze
Grundzüge des Thüringer Datenschutzgesetzes (ThürDSG)

Anlage 85

Veranstaltung der SPD Jena zur Vorratsdatenspeicherung
7. Juli 2015

Inhalt u. a.:
Das Grundrecht auf informationelle Selbstbestimmung
Die Vorratsdatenspeicherung – eine Beruhigungspille für das Volk?
Vorratsdatenspeicherung:
das Urteil des Bundesverfassungsgerichts vom 2. März 2010
das Urteil des Europäischen Gerichtshofs vom 8. April 2014
der Gesetzentwurf der Bundesregierung zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten

Anlage 86

E-Mail-Verschlüsselung für GnuPG und Outlook,
Kooperationsveranstaltung des ThILLM und des TLfDI
8. September 2015

Inhalt:
Vorbereitung
Schlüsselerzeugung
Schlüsseltausch
Schlüsselprüfung
Schlüsselnutzung

Anlage 87

„Datenschutz in sozialen Einrichtungen“
PARITÄTISCHE Akademie Thüringen
22. September 2015

Inhalt:
Warum Datenschutz?
Historischer Hintergrund
Rechtliche Grundlagen - Systematik
Allgemeine Grundsätze des Datenschutzes
Ermächtigungsgrundlagen
nach dem SGB
nach dem BDSG
nach dem ThürDSG
Technische und organisatorische Maßnahmen
Der TLfDI!

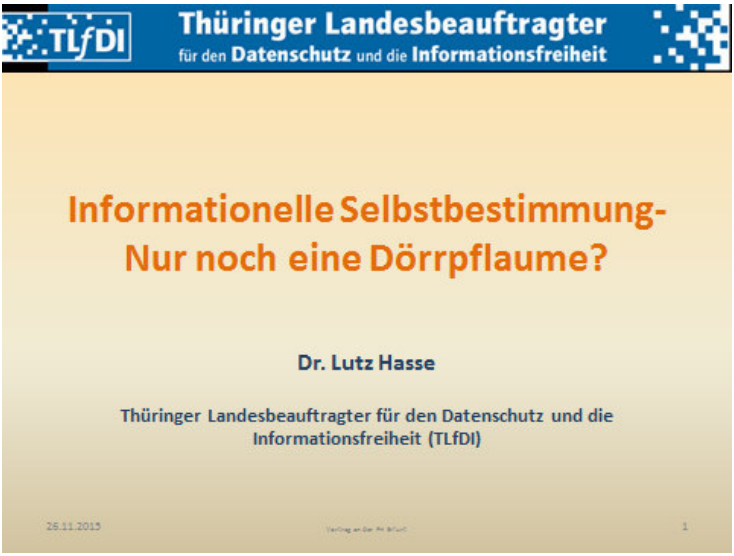
Anlage 88

Fachtagung der Kultusministerkonferenz KMK in Berlin
29. September 2015

Inhalt:
Datenschutz - Aktuelle Situation in Deutschland und Europa
Datenschutz als Aspekt digitaler Bildung
Datenschutz als Zukunftskompetenz – Was muss passieren?

Anlage 89

Fachhochschule Erfurt,
Angewandte Informatik
26. November 2015



Inhalt:
Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Europa
Privatsphäre – Warum?
Schlagabtausch

Abkürzungsverzeichnis

AbfWS	Satzung über die Vermeidung, Verwertung und Entsorgung von Siedlungsabfällen
Abs.	Absatz
AfV	Amt für Verfassungsschutz
AGB	Allgemeine Geschäftsbedingungen
AgrStatG	Agrarstatistikgesetz
ALG	Arbeitslosengeld
ANBest-P	Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung
Anm.	Anmerkung
AO	Abgabenordnung
App	Application software
ARMIN	Arzneimittelinitiative Sachsen-Thüringen
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
AufbewBest	Aufbewahrungsbestimmungen
AWB	Abfallwirtschaftsbetrieb
BAföG	Bundesausbildungsförderungsgesetz
BayLDA	Bayrisches Landesamt für Datenschutzaufsicht
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BEM	betriebliches Eingliederungsmanagement
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BNotO	Bundesnotarordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
BZ	Bildungszentrum
bzw.	beziehungsweise

d. h.	das heißt
DA-DAB	Dienstanweisung zur Behandlung von Aufsichtsbeschwerden gegen Angehörige der Thüringer Polizei im Geschäftsbereich der Landespolizeidirektion
DA-Diszi	Dienstanweisung zur Behandlung von Disziplinarangelegenheiten im Geschäftsbereich der Landespolizeidirektion
DolmV TH	Thüringer Verordnung zur Regelung der allgemeinen Beeidigung von Dolmetschern und der Ermächtigung von Übersetzern
DP AG	Deutsche Post AG
DSK	Datenschutzkonferenz
DSL	Digital Subscriber Line
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EHS	Ergänzendes Hilfesystem
eIDAS	electronic identification and trust services
ESF	Europäischer Sozialfond
EStG	Einkommensteuergesetz
EuGH	Europäischer Gerichtshof
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FBS-TH	Fallbearbeitungssystem Thüringen
GASt/Zst	Geldannahmestelle/Zahlstelle
gem.	gemäß
GewO	Gewerbeordnung
GFAW	Gesellschaft für Arbeits- und Wirtschaftsförderung
GFAW Thüringen	Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen
GG	Grundgesetz
ggf.	gegebenenfalls
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum
GKV-Modernisierungsgesetz	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung

– GMG	
HAMASYS	Haushaltsmanagementsystem
HWK	Handwerkskammer
i. d. R	in der Regel
i. V. m.	in Verbindung mit
ICF	Internationale Klassifikation der Funktionen
IfSG	Infektionsschutzgesetz
ITP	Integrierte Teilhabeplanung
JVA	Justizvollzugsanstalt
KAG	Kommunale Arbeitsgemeinschaft
Kita	Kindertagesstätte
KJÄD	Kinder- und Jugendärztlicher Dienst
KSJ	Kommunalservice Jena
KV	Kassenärztliche Vereinigung
LEG	Landesentwickungsgesellschaft
LFD	Landesfinanzdirektion
LfD	Landesbeauftragte für den Datenschutz
LoD	Level of Detail
LPD	Landespolizeidirektion
LPG	Landwirtschaftliche Produktionsgenossenschaften
LPI	Landespolizeiinspektion
MiStra	Anordnung über Mitteilung in Strafsachen
NSA	National Security Agency
o. g.	oben genannte
OBG	Ordnungsbehördengesetz
OH	Orientierungshilfe
OH KIS	Orientierungshilfe „Krankenhausinformationssysteme“
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten

PÄD	Polizeiärztlicher Dienst
PAG	Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei
PAuswG	Personalausweisgesetz
PC	Personal Computer
Rn.	Randnummer
Rz.	Randziffer
SaaS	Software as a Service
SARS	SYBORG Auskunfts- und Recherche-System
SGB	Sozialgesetzbuch
SHK	Saaleholzlandkreis
SigG	Signaturgesetz
StA	Staatsanwaltschaft
StAG	Staatsangehörigkeitsgesetz
StGB	Strafgesetzbuch
StOP	Strafprozessordnung
StPO	Strafprozessordnung
StVO	Straßenverkehrsordnung
SWE	Stadtwerke Erfurt
TAB	Thüringer Aufbaubank
TB	Tätigkeitsbericht
TFM	Thüringer Finanzministerium
ThAVel	Thüringer Antragsystem für Verwaltungsleistungen
Thoska	Thüringer Hochschul- und Studentenwerkskarte
ThürAbfG	Thüringer Gesetz über die Vermeidung, Verminderung, Verwertung und Beseitigung von Abfällen
ThürAG-BMG	Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes
ThürAGGVG	Thüringer Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
ThürArchivG	Thüringer Archivgesetz
ThürBestG	Thüringer Bestattungsgesetz

ThürBG	Thüringer Beamtengesetz
ThürBVVG	Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürBVVG	Thüringer Gesetz über Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürDG	Thüringer Disziplinargesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürFSO-SW	Thüringer Fachschulordnung für die Bildungsgänge im Sozialwesen
ThürGGO	Gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen
ThürGleichStatVO	Thüringer Gleichstellungsstatistikverordnung
ThürHeilBG	Thüringer Heilberufegesetz
ThürHG	Thüringer Hochschulgesetz
ThürJVollzGB	Thüringer Justizvollzugsgesetzbuch
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKiStG	Thüringer Kirchensteuergesetz
ThürKO	Thüringer Kommunalordnung
ThürKWO	Thüringer Kommunalwahlordnung
ThürLWG	Thüringer Landeswahlgesetz
ThürLWO	Thüringer Landeswahlordnung
ThürMeldeG	Thüringer Meldegesetz
ThürMRVG	Thüringer Maßregelvollzuggesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürPolPrüffristVO	Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung
ThürPsychKG	Thüringer Gesetz zur Hilfe und Unterbringung psychisch kranker Menschen
ThürSchfTG	Thüringer Gesetz über Schulen in freier Trägerschaft
ThürSchulG	Thüringer Schulgesetz
ThürSchul-	Thüringer Verordnung über die Schulgesundheits-

gespflVO	pflege
ThürStAnz	Thüringer Staatsanzeiger
ThürStatG	Thüringer Statistikgesetz
ThürUIG	Thüringer Umweltinformationsgesetz
ThürVerf	Verfassung des Freistaats Thüringen
ThürVerf	Verfassung des Freistaats Thüringen
ThürVerfGHG	Thüringer Verfassungsgerichtshof
ThürVerfSchG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürWTG	Thüringer Wohn- und Teilhabegesetz
THVPS	Verwaltungsplattform Schulwesen
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TKG	Telekommunikationsgesetz
TLFD	Thüringer Landesfinanzdirektion
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLKA	Thüringer Landeskriminalamt
TLS	Thüringer Landesamt für Statistik
TLVermGeo	Thüringer Landesamt für Vermessung und Geoinformation
TLVwA	Thüringer Landesverwaltungsamt
TMASGFF	Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie
TMBJS	Thüringer Ministerium für Bildung, Jugend und Sport
TMBLV	Thüringer Ministerium für Bau, Landesentwicklung und Verkehr
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kultur
TMG	Telemediengesetz
TMIK	Thüringer Ministerium für Inneres und Kommunales

TMIL	Thüringer Ministerium für Infrastruktur und Landwirtschaft
TMLFUN	Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz
TMMJV	Thüringer Ministerium für Migration, Justiz und Verbraucherschutz
TMSFG	Thüringer Ministerium für Soziales, Familien und Gesundheit
TMWAT	Thüringer Ministerium für Wirtschaft und Arbeit und Technologie
TMWWDG	Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft
TPG	Thüringer Pressegesetz
u. a.	unter anderem
u. U.	unter Umständen
UA	Untersuchungsausschuss
UAG	Thüringer Untersuchungsausschussgesetz
UAG	Unterarbeitsgruppe
UAK	Unterarbeitskreis
UKJ	Universitätsklinikums Jena
VBS	Vorgangsbearbeitungssystem
VG	Verwaltungsgemeinschaft
vgl.	vergleiche
VoBraWeb	Software zum vorbeugenden Brandschutz
VwGO	Verwaltungsgerichtsordnung
VwV VA-StVOWi	Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei
WoGG	Wohngeldgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

Sachregister

Notizen:

Notizen:

Notizen:

TLfDI
Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

2. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

Vorbemerkungen zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361/3771900, Telefax: 0361/3771904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: Druckhaus Gera GmbH
Jacob-A-Morand-Straße 16, 07552 Gera
Telefon: 0365/737520
E-Mail: info@druckhaus-gera.de

Redaktionsschluss: 17.05.2016

Bildnachweis: CD mit Adressen und Bankdaten inmitten Euro-Scheinen@Helmut Spoonwood - Fotolia

2. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2014 bis 31. Dezember 2015
Zitiervorschlag: 2. TB LfDI Thüringen

Der 2. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Mai 2016

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Entschließungen der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Entschließungen der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am am 30. September/1. Oktober 2015 in Darmstadt

Entschließung der Sondersitzung der Datenschutzbeauftragten des Bundes und der Länder am 21. Oktober 2015 in Frankfurt

Pressemitteilungen 2014

Pressemitteilungen 2015

Vorträge und Veranstaltungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

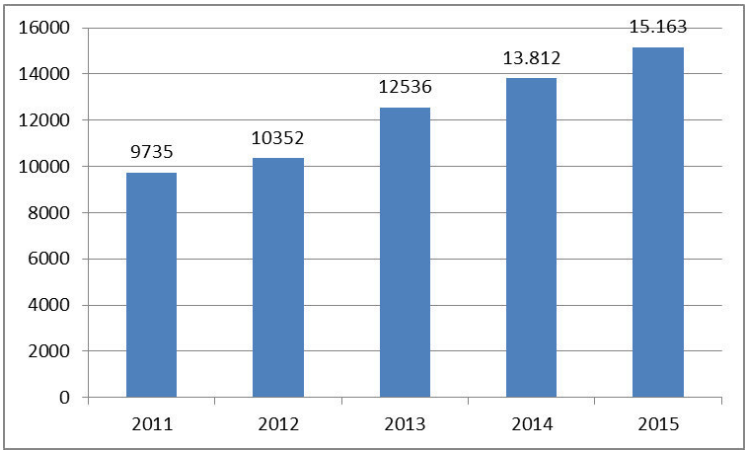
B Nicht-öffentlicher Bereich

Vorwort

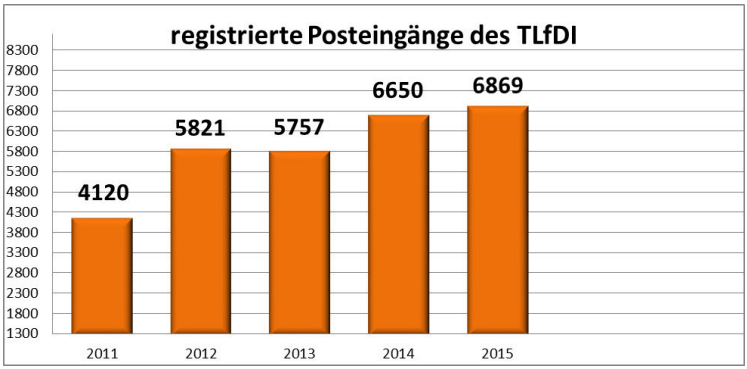
Dr. Lutz Hasse

Gleich auf den ersten Blick zeigt der Umfang des 2. Tätigkeitsberichts im nicht-öffentlichen Bereich, dass der Arbeitsanfall beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter angewachsen ist. Der Tätigkeitsbericht wird immer dicker! Die immense Zahl der Beiträge machte es sogar notwendig, dass der Tätigkeitsbericht für den nicht-öffentlichen Bereich und der 11. Tätigkeitsbericht für den öffentlichen Bereich in zwei gesonderten Bänden veröffentlicht werden. Für

den nicht-öffentlichen Bereich gibt es erstmals einen separaten Band. Einen großen Teil der Arbeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im nicht-öffentlichen Bereich stellte die datenschutzrechtliche Prüfung von Videoüberwachungsanlagen in Thüringen dar (s. dazu auch Beitrag Nummer 1). Manche Beiträge finden sich wegen der allgemeinen Bedeutung in beiden Bänden.
Vorab sei angemerkt, dass sich die Beiträge nahezu ausschließlich auf den Berichtszeitraum beziehen. Wenn es nach dem Ende des Berichtszeitraums eine wesentliche Änderung gegeben hat, gibt es einen entsprechenden Hinweis.
Insgesamt wurden beim TLfDI im Berichtszeitraum 28.975 Dokumente im Dokumentenmanagementsystem erstellt (13.812 im Jahr 2014 und 15.163 im Jahr 2015). Vergleicht man diese Zahlen mit denjenigen der letzten Jahre seit Einführung des Dokumentenmanagementsystems, ist ein kontinuierlicher Anstieg zu verzeichnen.



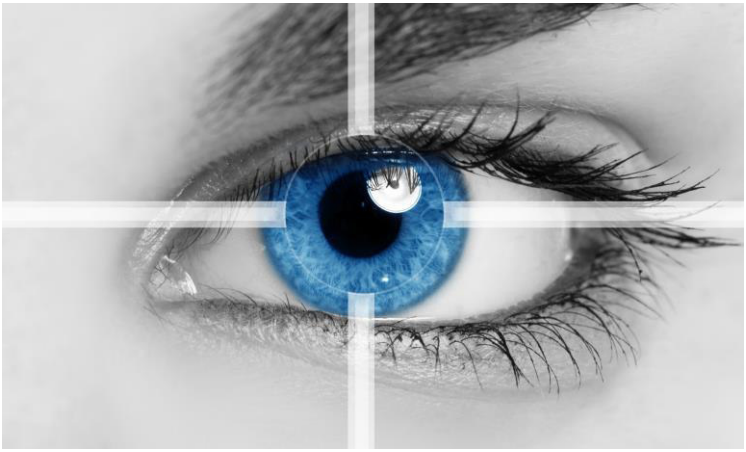
Diese Zahlen erfassen alle beim TLfDI elektronisch angelegten Dokumente, also Posteingänge und Postausgänge sowie interne Vermerke.
Sieht man sich lediglich die Posteingänge an, ergibt sich ein ähnliches Bild:



Auch in den Jahren 2014/2015 ist die personelle Situation der Behörde nach wie vor äußerst angespannt. Aufgrund der wachsenden Zahl der Eingaben und auch wegen der zunehmenden Komplexität datenschutzrechtlicher Fragestellungen kommt die Behörde immer wieder an ihre Grenzen. Im nicht-öffentlichen Bereich kommt hinzu, dass die Behörde hier im Ordnungswidrigkeitenverfahren und wenn sie im Verwaltungsverfahren Anordnungen trifft an ein förmliches Verfahren gebunden ist. Gegen ihre Entscheidungen können und werden Rechtsmittel eingelegt. Das macht die Verfahren komplizierter und langwieriger. Anlassunabhängige Kontrollen sind daher nur noch in begrenztem Umfange möglich, und die Bearbeitung von Anfragen und Beschwerden kann leider nicht immer zeitnah erfolgen. Trotzdem ist festzustellen, dass die Mitarbeiter der Behörde hochmotiviert alle Beschwerden, egal, ob sie namentlich oder anonym erhoben werden, bearbeiten und allen Hinweisen nachgehen. Daher möchte ich mich an dieser Stelle ausdrücklich bei meinen Mitarbeitern bedanken, die sehr oft „am Anschlag“ arbeiten und ohne deren unermüdlichen Einsatz es um den Datenschutz in Thüringen wesentlich schlechter bestellt wäre. Die Arbeit wird dabei nie zur Routine, weil die technische Entwicklung immer neue Datenschutzfragen aufwirft. Hinzu kommt, dass mit dem baldigen Inkrafttreten der Datenschutzgrundverordnung der Europäischen Union neue Herausforderungen auf den TLfDI zukommen. Da die Datenschutzgrundverordnung unmittelbar gelten wird, ist ein Großteil des bislang geltenden Bundesdatenschutzgesetzes Makulatur. Die Unternehmen in Thüringen müssen die Anforderungen der neuen Regelungen umsetzen und der TLfDI wird sie hierbei tatkräftig unterstüt-

zen. Daher muss die ganze Behörde sich bereits vorher mit den neuen Regelungen vertraut machen. Deutlich zeichnet sich ab: Die Arbeit wird nicht weniger, sondern schnell mehr. Soll die Leistungsfähigkeit der Behörde langfristig erhalten bleiben, bedarf es dringend einer Aufstockung des Personals. Auf die weitere Förderung durch die Landtagsfraktionen muss und darf der TLfDI vertrauen.

Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: https://www.tlfdi.de/tlfdi/). Dadurch kann auf Geräten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden Software der Link durch das Gerät wieder decodiert werden und so können „Abschreibfehler“ vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers „Marty Mouse“ in der Version 1.0 empfohlen werden, da hier Open Source Software genutzt wird und die App nur minimale Funktionen besitzt. Für iOS ist dem TLfDI keine datenschutzgerechte App bekannt.



Eye close-up – © Minerva Studio / Fotolia.com

1 Schwerpunkte im Berichtszeitraum

Einen großen Teil der Arbeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im nicht-öffentlichen Bereich stellte die datenschutzrechtliche Prüfung von Videoüberwachungsanlagen in Thüringen dar. Dies betraf die Videoüberwachung von Mitarbeitern, Kunden, Nachbarn oder auch unbeteiligten Dritten. Hierzu wird auf die zahlreichen Berichte zur Videoüberwachung im Bericht verwiesen. Als arbeitsintensiv erwiesen sich insbesondere die Fälle, in denen sehr viel Videotechnik mit teilweise mehr als 100 Kameras zum Einsatz kam. Viele Beschwerden gab es auch im Bereich des Beschäftigtendatenschutzes. Die fortschreitende Technologisierung der Arbeitswelt ermöglicht es dem Arbeitgeber, auf immer leichterem Weg Mitarbeiter zu überwachen. Zu nennen sind hier die Datenerhebung im Rahmen von Logistikprozessen oder GPS-Tracking. Auch in diesem Bereich hat der TLfDI nach Hinweisen schwerpunktmäßig Unternehmen geprüft.
Zu nennen ist auch die Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015. Seit dem Tag der Entscheidung wechselten sich Abstimmungen, E-Mails über neueste Entwicklungen und Termine sowie Sondersitzungen der Datenschutzkonferenz im Tagesrhythmus ab. Zu klären war, welche Rechtsgrundlagen Betriebe nach dem EuGH-Urteil, das die Safe-Harbor-Entscheidung für nichtig erklärt

hatte, alternativ für Datenübermittlungen in die USA nutzen konnten (siehe dazu im Einzelnen Anlage 23).
Seit Ende Februar 2016 ist nunmehr mit "Privacy Shield" das geplante Nachfolgeabkommen zu "Safe-Harbor" bekannt. Die Art. 29-Datenschutzgruppe der Europäischen Datenschutzbeauftragten hält aber auch die "Privacy-Shield"-Regelungen an mehreren Stellen für mit dem europäischen Datenschutzstandard nicht vereinbar.
Im Bereich der Technik ist die Cyberkriminalität auf dem Vormarsch. Zwei Trends sind zu erkennen: Seit Jahren versuchen Hacker private Rechner zu kapern, um Daten auf den Rechnern auszuspionieren, die elektronische Kommunikation mitzulesen oder zu manipulieren oder die Rechner für einen gemeinsamen programmierten Angriff zu nutzen (Bot-Netze). Hilfe für die Bürger seitens des Staates gab es bis dato kaum. Erst mit den Hackerangriffen auf Behördenstrukturen und Wirtschaftsunternehmen erfolgte ein Umdenken der Politik und man kreierte die „Cyber-Sicherheitsstrategie“. Dem folgte ein IT-Sicherheitsgesetz, welches nun die Erhöhung der Sicherheit in informationstechnischen Systemen regelt. So wurden als kritische Infrastrukturen und damit als besonders schutzwürdig Sektoren der Energie, der Informationstechnik und Telekommunikation, des Transportes und des Verkehrs, der Gesundheit, des Wassers, der Ernährung sowie des Finanz- und Versicherungswesens definiert (siehe Nummer 14.5). Mit dem Ergebnis, dass Diensteanbieter nunmehr die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden dürfen, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Der Schutz für die Bürger und ihre Daten bleibt dabei aber weiterhin auf der Strecke.

Papierschnitzel Stichwort Kundenliste – © Gina Sanders / Fotolia.com

2 Allgemeine Datenschutzprobleme in Unternehmen

2.1 Safe Harbor – Anlegen verboten

Der 6. Oktober 2015 war ein guter Tag für den Datenschutz. Die Luxemburger Richter des Europäischen Gerichtshofes (EuGH) urteilten, dass die Entscheidung der Europäischen Kommission vom 26. Juli 2000 (2000/520/EG) über die Gewährung eines angemessenen Datenschutzniveaus auf der Grundlage des Safe-Harbor-Abkommens (Übersetzung wörtlich: „Sicherer-Hafen-Abkommen“) für Übermittlungen von Daten in die USA keine Gültigkeit mehr besitze (Az.: C-362/14).
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowie die anderen Datenschutzbeauftragten des Bundes und der Länder hatten bereits nach den Enthüllungen von Edward Snowden im Sommer 2013 immer wieder die Aussetzung der Übermittlung personenbezogener Daten auf der Grundlage des Safe-Harbor-Abkommens gefordert, da nach Ansicht der deutschen Datenschutzbeauftragten das Abkommen keinen ausreichenden Schutz vor Eingriffen in das Grundrecht auf informationelle Selbstbestimmung durch die amerikanischen (Sicherheits-)Behörden

biete. Die USA verfügten demnach nicht über ein für europäische Standards notwendiges angemessenes Datenschutzniveau. Dies wurde nunmehr durch die Richter des EuGH bestätigt. Als Folge des Urteils wird der TLfDI zunächst die Übermittlung von personenbezogenen Daten, die sich ausschließlich auf das Safe-Harbor-Abkommen stützen, untersagen und gegebenenfalls mit den ihm zur Verfügung stehenden Mitteln ahnden.
Im Lichte des EuGH-Urteils sind aber darüber hinaus auch die Datenübermittlungen in die USA, basierend auf EU-Standardvertragsklauseln oder sogenannten verbindlichen Unternehmensregelungen (auf Englisch: Binding Corporate Rules = BCR), höchst fraglich geworden. In jedem Fall werden die deutschen Datenschutzbehörden keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von BCR oder Datenexportverträgen erteilen. Zu klären ist auch, ob und inwieweit Datenübermittlungen aufgrund einer Einwilligung der Betroffenen vorgenommen werden können.
Der EuGH stellte in seinem Urteil weiter fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten unabhängig von der Entscheidung der Kommission nicht daran gehindert sind, die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen. Schwierig wird es jedoch, die Entscheidungen der Kommission rechtlich anzugreifen, da den Datenschützern bisher kein eigenes Klagerecht zur Verfügung steht. Hier ist – so der EuGH – der Gesetzgeber gefordert, ein entsprechendes Klagerecht gesetzlich zu verankern.
Diese und weitere Punkte wurden auf einer Sondersitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) am 21. Oktober 2015 in einem Positionspapier zusammengetragen (s. Anlage 17).
Die „Schonfrist“ für Unternehmen, ihre Arbeitsabläufe entsprechend datenschutzkonform anzupassen bzw. neu zu regeln, lief bis zum 31. Januar 2016 und wurde dann noch einmal bis zum 29. Februar 2016 verlängert. Das mittlerweile von der EU-Kommission vorgelegte geplante „Privacy-Shield“-Abkommen wird aber nicht nur von der Artikel 29-Datenschutzgruppe als dringend nachbesserungswürdig erachtet. Die Kompetenzen und die Unabhängigkeit einer Ombudsperson für datenschutzrechtliche Belange von EU-Bürgerinnen und Bürgern in den USA erscheinen dabei ebenso fraglich wie die weiterhin mögliche massenhafte Datenspeicherung von US-

Geheimdiensten. Stürmische Zeiten im Datenschutzrecht bleiben uns daher wohl erhalten.

Mit dem Safe-Harbor-Urteil hat der Europäische Gerichtshof eine klare Linie aufgezeigt. Datenübermittlungen in die USA auf der Grundlage des Safe-Harbor-Abkommens sind unzulässig. Insbesondere Unternehmen sollten nun schnellstmöglich ihre Verfahren zum Datentransfer überprüfen und datenschutzgerecht gestalten. Inwieweit Datenübermittlungen auf der Grundlage von EU-Standardvertragsklauseln, BCR oder aufgrund der Einwilligung der Betroffenen weiterhin zulässig sind, wird sich im Jahr 2016 zeigen.

2.2 Genaue Prüfung bei Recyclingunternehmen – und deren Kosten

Im ersten Tätigkeitsbericht (TB) zum Datenschutz im nicht-öffentlichen Bereich berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass im damaligen Berichtszeitraum diverse Recyclingunternehmen kontrolliert worden waren (vergleiche im letzten TB Nr. 3.11). Nicht alle Kontrollen konnten im 1. Berichtszeitraum abgeschlossen werden. Bei einem Unternehmen wurden zahlreiche datenschutzrechtliche Mängel festgestellt. So hatte der bestellte betriebliche Datenschutzbeauftragte (bDSB) keine speziellen Datenschutzkenntnisse. Der TLfDI forderte daher, dass der betriebliche Datenschutzbeauftragte eine Fortbildung besucht, in welcher Datenschutzkenntnisse erworben werden können. Der Betrieb hatte zudem seine Lohnbuchhaltung auf ein externes Unternehmen übertragen, ohne einen Vertrag geschlossen zu haben, der den gesetzlichen Anforderungen an eine Auftragsdatenverarbeitung entsprach. Auch gab es im Unternehmen keine schriftlichen Festlegungen zu technischen und organisatorischen Maßnahmen nach § 9 Bundesdatenschutzgesetz. Der TLfDI empfahl, Regelungen zu folgenden Sachverhalten zu treffen: zum Datenschutz, zur Nutzung der Arbeitsplätze mit IT-Unterstützung, zum Umgang mit Telefon, E-Mail und Internet, insbesondere zu deren privater Nutzung, Berechtigung-/Zugriffsregelungen für Fachanwendungen, zur Gestaltung von Passwörtern, Regelungen zur Datensicherung, zum IT-Notfallkonzept, zur Entsorgung von Akten und Datenträgern, zum Zugang für die verschiedenen Diensträume, zur Schlüsselordnung sowie die Erstellung eines Lösch- und Sperr-

konzepts. Auch die im Unternehmen vorhandenen vier Kameras wurden datenschutzrechtlich geprüft. Der TLfDI forderte, die Speicherdauer der Aufnahmen zu begrenzen, Hinweisschilder zur Videoüberwachung anzubringen, die Kameras datenschutzgerechter auszurichten bzw. bei einer Kamera, diese nur zu Nachtzeiten zu aktivieren. Außerdem forderte der TLfDI, dass bei der Schrottabgabe keine vollständigen Personalausweiskopien mehr gefordert und erstellt werden (siehe hierzu auch Nummer 2.27). Nach vielfältigem Schriftverkehr reichte die kontrollierte Stelle die erforderlichen Unterlagen nach und kam auch ansonsten im Laufe des Verfahrens den Forderungen des TLfDI nach. Damit konnte das Verfahren abgeschlossen werden, dessen Kosten das kontrollierte Unternehmen zu tragen hatte, da bei der Kontrolle Mängel festgestellt worden waren.

Wenn bei der Kontrolle eines Unternehmens Mängel festgestellt werden, hat dieses die Kosten der Kontrolle zu tragen, auch wenn es alle Forderungen des TLfDI erfüllt, § 42 Abs. 4 Satz 2 Thüringer Datenschutzgesetz.

2.3 Kontoauszüge – ausnahmsweise ungeschwärzt bei Förderung aus dem Europäischen Sozialfonds

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines Zuwendungsempfängers aus Mitteln des Europäischen Sozialfonds und/oder des Freistaats Thüringen zur Förderung betriebswirtschaftlicher und technischer Beratungen von kleinen und mittleren Unternehmen und Existenzgründern (Beratungsrichtlinie). Dabei hatte sich der TLfDI mit der Frage auseinanderzusetzen, inwieweit ein Unternehmen berechtigt ist, von dem Beschwerdeführer die Abgabe eines Kontoauszugs im Original ohne Schwärzung anzufordern.
Daraufhin forderte der TLfDI die Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW) auf, mitzuteilen, nach welcher Regelung der aufgeführten Beratungsrichtlinie ungeschwärzte Kontoauszüge verlangt werden können.
Nach Ziffer 7.4.1 Satz 3 der Richtlinie über die Gewährung von Zuschüssen aus Mitteln des Europäischen Sozialfonds und/oder des Freistaats Thüringen zur Förderung betriebswirtschaftlicher und technischer Beratungen von kleinen und mittleren Unternehmen und

Existenzgründern (Beratungsrichtlinie) sind Originalbelege beizufügen. Die GFAW teilte daraufhin dem TLfDI mit, dass Sie nicht auf ungeschwärzte Kontoauszüge bestehe. Nach Prüfung teilte dann der TLfDI dem Beschwerdeführer mit, dass die zugrunde liegende Richtlinie eindeutig sei. Die GFAW verlange nach deren Aussage im Rahmen des Verfahrens über den Verwendungsnachweis jedoch keine ungeschwärzten Kontoauszüge, soweit die zu prüfenden Informationen klar erkennbar seien. Schließlich wies der TLfDI den Beschwerdeführer noch darauf hin, dass bei Schwärzung der Originalbelege unter Umständen gegen Vorschriften der ordnungsgemäßen Buchführung verstoßen werden könnte. Der Beschwerdeführer bedankte sich beim TLfDI und sah dieses Verfahren für ihn als erledigt an. Im Ergebnis ist daher aufgrund dieser Spezialregelung die von dem Unternehmen geforderte Übermittlung ungeschwärzter Kontoauszüge der Zuwendungsempfänger im Rahmen des Verfahrens über Verwendungsnachweise und deren Überprüfung nicht als Verstoß gegen datenschutzrechtliche Bestimmungen anzusehen.

Nach Ziffer 7.4.1 Satz 3 der Richtlinie über die Gewährung von Zuschüssen aus Mitteln des Europäischen Sozialfonds und/oder des Freistaats Thüringen zur Förderung betriebswirtschaftlicher und technischer Beratungen von kleinen und mittleren Unternehmen und Existenzgründern (Beratungsrichtlinie) sind im Rahmen des Verfahrens über den Verwendungsnachweis die entsprechenden Nachweisbelege als Original zum Zwecke der Prüfung beizulegen. Das Anfordern eines Kontoauszugs im Original ist im Rahmen dieses Fördermittelverfahrens daher ausnahmsweise zulässig.

2.4 Geld waschen in Deutschland – Immobilienmakler trifft Auskunftspflicht

Das Geldwäschegesetz verpflichtet Makler zur Mitarbeit: Um kriminelle Strukturen und Terrorismus zu bekämpfen, haben Makler eine umfassende interne und externe Dokumentationspflicht über ihre Kundenkontakte.
Im Frühjahr erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu diesem Thema eine Anfrage der Industrie- und Handelskammer Ostthüringen (IHK-Ost) zu Gera. Hintergrund war, dass das Thüringer Landesverwaltungsamt (TLVwA) mit einem Auskunftsbogen für den Bereich

Immobilienmakler Daten auf Grundlage des Geldwäschegesetzes erhob. Namens ihrer Mitgliedsunternehmen bat die IHK-Ost den TLfDI um Klärung der datenschutzrechtlichen Zulässigkeit der Datenerhebung. Insbesondere hielt die IHK-Ost die Abfrage nach dem durchschnittlichen Jahresumsatz und durchschnittlichen Jahresgewinn für unzulässig. Außerdem bemängelte die IHK-Ost noch die fehlende Belehrung über das Auskunftsverweigerungsrecht im Sinne des § 16 Abs. 4 Geldwäschegesetz (GWG) durch das TLVwA. Der TLfDI bat daraufhin das TLVwA als zuständige Aufsichtsbehörde im Sinne des § 16 Abs. 2 Nr. 9 GWG um schriftliche Stellungnahme zur Erforderlichkeit der Datenerhebung über den durchschnittlichen Jahresumsatz sowie den durchschnittlichen Jahresgewinn in Bezug zur Aufsichtstätigkeit nach GWG.
Das TLVwA teilte mit, dass § 16 Abs. 3 GWG Rechtsgrundlage für die Abfrage der oben genannten Daten sei. Die Vorschrift erlaube es unter anderem, unentgeltlich Auskünfte über alle Geschäftsangelegenheiten von den nach dem GWG Verpflichteten zu verlangen, die für die Einhaltung der im GWG festgelegten Anforderungen von Bedeutung und damit erforderlich sind. Nach § 2 Abs. 1 Nr. 10 GWG seien Immobilienmakler Verpflichtete im Sinne dieses Gesetzes. Welche Informationen das TLVwA für die Erfüllung seiner Aufgaben als Aufsichtsbehörde nach dem GWG benötige, lege dieses im Rahmen einer Ermessensentscheidung fest.
Das TLVwA führte gegenüber dem TLfDI aus, dass gerade im Hinblick auf den risikobasierten Ansatz des Geldwäschegesetzes diese Informationen für die Aufsichtsbehörde erforderlich wären, um die von dem jeweiligen Unternehmen konkret getroffenen, geldwäscherechtlichen Maßnahmen adäquat bewerten zu können. Nach Auswertung der vom TLVwA erteilten Auskünfte erfolge eine Einordnung der Gewerbebetriebe in Risikokategorien zur Abschätzung des Geldwäscherisikos der jeweiligen Unternehmen. Diese Einteilung in Risikokategorien basiere bei Immobilienmaklern unter anderem auf Umsatz- und Gewinnangaben, der Größe des Unternehmens, der Anzahl von Geschäften in Höhe des gegenwärtigen 15.000 Euro-Schwellenwertes und der Korrelation dieser Daten miteinander. Hierbei auftretende Unschlüssigkeiten (beispielsweise ein sehr kleines Unternehmen verfügt über einen sehr hohen Umsatz oder Umsatz und Anzahl der Geschäfte stehen in keinem nachvollziehbaren Verhältnis) flössen in die Risikobemessung des Unternehmens im Sinne des GWG ein.

Nach Prüfung der Sach- und Rechtslage war den Ausführungen des TLVwA zuzustimmen, soweit sie Aufgabenbereich und Zuständigkeit betrafen. Die Ausführungen, warum welche Daten durch das TLVwA erhoben wurden, erschienen nachvollziehbar. Der TLfDI kann, wenn die vorgebrachten Gründe plausibel erscheinen, im Rahmen seiner Befugnisse eine solche Ermessensentscheidung nur auf Nicht- oder Fehlgebrauch des Ermessens hin überprüfen. Ein solcher war nicht feststellbar.
Hinsichtlich der fehlenden Belehrung über das Auskunftsverweigerungsrecht durch das TLVwA stellte der TLfDI fest, dass das Fehlen der Belehrung keine Auswirkungen auf die Zulässigkeit der Erhebung der Daten hatte. Es handelt sich hierbei um eine so genannte Kollisionsauflösungsnorm, deren Zweck es ist, im Verwaltungsverfahren gewonnene Kenntnisse in ein gegebenenfalls eingeleitetes Bußgeldverfahren zu übertragen. Schreibt eine solche Kollisionsauflösungsnorm eine Belehrung vor, führt deren Fehlen lediglich zu einer Unverwertbarkeit der so gewonnenen Informationen in einem eventuell folgenden Bußgeldverfahren nach dem GWG.

Nach § 16 Abs.3 Satz 1 GwG hat ein Verpflichteter, beispielsweise ein Immobilienmakler, der zuständigen Aufsichtsbehörde auf Verlangen Auskünfte über alle Geschäftsangelegenheiten zu erteilen und Unterlagen vorzulegen, die für die Einhaltung der im Geldwäschegesetz festgelegten Anforderungen von Bedeutung sind.

2.5 Erlaubt oder nicht? Kundenwerbung durch Immobilienmakler

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Wohnungseigentümers über die Nutzung der Anschriften sämtlicher Miteigentümer einer Wohnungseigentumsgemeinschaft (WEG) an eine Immobilien- und Hausverwaltung. Auf welchem Weg diese Verwaltung an die Daten gekommen war, war ebenfalls unbekannt. Die Daten wurden genutzt, um die Mitglieder der WEG anzuschreiben und diesen ein Angebot über die Verwaltung der Immobilie zu unterbreiten. Auf Nachfrage des Beschwerdeführers über die Herkunft seiner bzw. der Miteigentümerdaten bei der Immobilien- und Hausverwaltung nach § 34 Bundesdatenschutzgesetz (BDSG) wurde ihm keine Auskunft erteilt.

Dieses Verhalten der Immobilien- und Hausverwaltung ist mit dem BDSG nicht vereinbar. Die verantwortliche Stelle hat gemäß § 34 Abs. 1 BDSG dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten und deren Herkunft zu erteilen. Zur Klärung des Sachverhalts forderte der TLfDI die Immobilien- und Hausverwaltung zur Stellungnahme zu den aufgeworfenen Fragen auf, insbesondere aber zur Beantwortung des Auskunftsersuchens des Bürgers. Daraufhin teilte die Haus- und Immobilienverwaltung unter Vorlage einer Hausvertretervollmacht dem TLfDI mit, dass Sie zur Wahrnehmung aller Rechtsgeschäfte und zur Vertretung des Sondereigentums von einem Miteigentümer der WEG bevollmächtigt sei. Darüber hinaus beinhalte die Vollmacht die Berechtigung zur Abgabe von verbindlichen Erklärungen im Namen dieses Miteigentümers. Aus dieser Vertretung des Sondereigentums für einen Miteigentümer der WEG und der damit verbundenen Rechte habe sie Kenntnis über die o.g. persönlichen Daten sämtlicher Mitglieder der WEG erhalten. Die geforderte Auskunftserteilung an den Bürger wurde ebenfalls vorgenommen und gegenüber dem TLfDI nachgewiesen.
Die datenschutzrechtliche Prüfung seitens des TLfDI ergab, dass die Haus- und Immobilienverwaltung zu Recht Kenntnis über sämtliche persönliche Daten und Anschriften der Miteigentümerdaten der WEG hatte. Nach § 24 Abs. 6 Satz 3 Wohnungseigentumsgesetz (WoEigG) ist jeder Wohnungseigentümer berechtigt, die Niederschriften einzusehen. Gemäß § 24 Abs. 7 Satz 8 WoEigG ist einem Wohnungseigentümer oder einem Dritten, den ein Wohnungseigentümer ermächtigt hat – wie vorliegend die Haus- und Immobilienverwaltung –, auf sein Verlangen Einsicht in die Beschlusssammlung zu geben. Daher hat jeder Wohnungseigentümer einen Anspruch auf Gewährung von Einsicht in sämtliche Verwaltungsunterlagen. Das Einsichtsrecht unterliegt keinen weiteren Voraussetzungen wie z. B. einem besonderen rechtlichen Interesse des Wohnungseigentümers oder einer Ermächtigung durch die übrigen Wohnungseigentümer. Nur das Verbot des Rechtsmissbrauchs (242 BGB) und das Schikaneverbot (§ 226 BGB) begrenzen das Einsichtsrecht (vergleiche dazu BGH, Urteil vom 11. Februar 2011, V ZR 66/10).
Daher war es zulässig, dass dem Miteigentümer und dessen Verwaltung für sein Sondereigentum sämtliche Eigentümerdaten aus dem Grundbuchblatt sowie aus den Anwesenheitslisten der vergangenen Eigentümerversammlungen vorlagen.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Erhebung und Speicherung personenbezogener Daten für die Erfüllung der Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an den Ausschluss der Verarbeitung oder Nutzung überwiegt. Das Einsichtsrecht der Haus- und Immobilienverwaltung in die Eigentümerdaten aus dem Grundbuchblatt und in die Anwesenheitslisten ergab sich aufgrund ordnungsgemäßer Bevollmächtigung durch den Miteigentümer der WEG und zur Erfüllung des Vertrages mit diesem. Die Interessen der übrigen Eigentümer können dieses Interesse an den Daten auch nicht überwiegen. Vielmehr muss ein Miteigentümer wissen, wer die sonstigen Miteigentümer sind. Der TLfDI konnte in diesem Punkt keinen datenschutzrechtlichen Verstoß der Haus- und Immobilienverwaltung in Bezug auf die Erhebung und Speicherung dieser Informationen zum Zweck der Verwaltung des Sondereigentums des Miteigentümers feststellen.
Damit war zwar die eigentliche Beschwerde abgearbeitet, jedoch stand ein weiterer Verstoß gegen das BDSG im Raum. Denn selbst, wenn das Erheben und Verarbeiten für die Erfüllung der Verwaltung des Sondereigentums erforderlich war, heißt das noch lange nicht, dass diese Daten für alle möglichen Zwecke genutzt werden können. So ist das Anschreiben der einzelnen WEG-Mitglieder als Werbeanschreiben einzustufen. Die Nutzung von personenbezogenen Daten zu Zwecken der Werbung wiederum ist jedoch den Grenzen des BDSG unterworfen.
Die Prüfung des Sachverhalts in Bezug auf das Werbeanschreiben ist bislang noch nicht abgeschlossen. Nach den dem TLfDI vorliegenden Informationen erfüllt das Werbeanschreiben nicht die vom Gesetz geforderten Voraussetzungen für eine datenschutzrechtlich einwandfreie werbliche Ansprache. Denn grundsätzlich ist Werbung nur mit der Einwilligung der Beworbenen zulässig, § 28 Abs. 3 Satz 1 BDSG. Dazu gibt es zwar umfassende Ausnahmen, die aber an bestimmte Voraussetzungen gekoppelt sind. So ist nach § 28 Abs. 3 Satz 2 BDSG die Verarbeitung oder Nutzung personenbezogener Daten ohne Einwilligung dann zulässig, wenn es sich nur um so genannte Listendaten handelt, wie hier der Fall. Jedoch ist dabei § 28 Abs. 3 Satz 2 zweiter Halbsatz Ziffer 1 bis 3 BDSG zu beachten, dessen Voraussetzungen hier nicht erfüllt waren. Danach darf die verantwortliche Stelle zwar für eigene Angebote ohne Ein-

willigung der Betroffenen werben, jedoch müssen die Daten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG beim Betroffenen erhoben worden sein, um mit diesem ein Schuldverhältnis zu begründen, durchzuführen oder zu beenden. Der Verwalter hatte mit den übrigen Mitgliedern der WEG jedoch keine geschäftliche Beziehung. Das Verfahren ist noch nicht abgeschlossen; über den Ausgang des Verfahrens wird der TLfDI berichten.

Ein Einsichtsrecht einer Haus- und Immobilienverwaltung zum Zweck der Verwaltung des Sondereigentums in die Eigentümerdaten aus dem Grundbuchblatt und in die Anwesenheitslisten ergibt sich aus einer ordnungsgemäßen Hausvertretervollmacht. Die Erhebung und Speicherung dieser Informationen ist für die Erfüllung der Geschäftszwecke der Immobilien- und Hausverwaltung im Zusammenhang mit der Verwaltung des Sondereigentums eines Miteigentümers gemäß § 28 Abs. 1 Nr. 2 BDSG zulässig. Die Speicherung und Nutzung der Daten weiterer Miteigentümer der WEG zum Zweck der werblichen Ansprache durch eine bevollmächtigte Haus- und Immobilienverwaltungen für Sondereigentum eines einzelnen Miteigentümers ist im Sinne des BDSG nicht zulässig. Zu Werbezwecken dürfen Daten nur genutzt werden, wenn das BDSG dies zulässt.

2.6 Problem: Muttizettel

Muttizettel. Umgangssprachlich steht dies für die Vereinbarung zwischen einer personensorgeberechtigten Person, also hier in aller Regel einem Elternteil und einer dritten volljährigen Person, über die Wahrnehmung von Erziehungsaufgaben als erziehungsbeauftragte Person für einen bestimmten Zeitraum, § 1 Abs. 1 Nr. 4 Jugendschutzgesetz (JuSchG). Sinn und Zweck eines solchen Muttizettels ist es z. B., Jugendlichen unter 16 Jahren die Teilnahme an einer Tanzveranstaltung (Disco) in Begleitung eines Erwachsenen zu ermöglichen, ohne dass der Veranstalter gegen das Jugendschutzgesetz verstößt, § 5 JuSchG.
Neben den vielen vermeintlichen Problemen, die diese Regelungen bei Jugendlichen verursachen, haben auch die Veranstalter die eine oder andere Schwierigkeit hiermit. Ein Discobetreiber wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um ein solches Problem zu klären. Nach Auffassung des Discobetreibers sei man nach Abschluss der

Tanzveranstaltung verpflichtet, die Muttizettel datenschutzgerecht zu entsorgen. Dies berge allerdings die Gefahr, so der Discobetreiber, dass Erziehungsberechtigte im Nachhinein den Vorwurf erheben könnten, dass ein Jugendlicher möglicherweise ohne eine solche Erlaubnis an der Tanzveranstaltung teilgenommen haben könnte. Bei Ermittlungen der zuständigen Aufsichtsbehörde (Jugendamt) könne man sich dann nicht mehr dieses Vorwurfs durch Vorlage des Muttizettels erwehren. Die Stadt riet dem Discobetreiber, sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden. Die Stadt, so der Fragesteller, wäre über die Möglichkeit einer Aufbewahrung von einem Jahr sehr glücklich, da die Bearbeitung von Ordnungswidrigkeiten in diesem Bereich einige Zeit in Anspruch nehmen würde.

Rechtlich betrachtet ist das Aufbewahren der Muttizettel eine Speicherung, das anschließende datenschutzgerechte Wegwerfen eine Löschung, § 3 Abs. 4 Bundesdatenschutzgesetz (BDSG). Insgesamt spricht man von einer Verarbeitung von personenbezogenen Daten. Hierfür benötigt der Discobetreiber eine Rechtsgrundlage, da das BDSG eine Verarbeitung nur dann zulässt, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG.

Hier besteht ein besonderes Interesse des Discobetreibers, den Zettel aufzubewahren, nämlich um sich möglicherweise gegenüber dem Jugendamt zu rechtfertigen, warum er einen 15-Jährigen in die Disco gelassen hat. Schutzwürdige Interessen der Betroffenen überwiegen in diesem Fall auch nicht. Aufbewahren darf der Discobetreiber diese Muttizettel nicht nur ein Jahr, sondern drei Jahre. Das hat einen einfachen Grund. Die Verstöße gegen das Jugendschutzgesetz verjähren in diesen Fällen nach drei Jahren ab der angeblichen Tatbegehung, § 31 Abs. 2 Nr. 1 Ordnungswidrigkeitengesetz. So lange muss sich der Betreiber auch gegen ein eventuelles Ordnungswidrigkeitenverfahren verteidigen können. Erst danach müssen diese Muttizettel datenschutzgerecht vernichtet werden. Dann aber wirklich!

Auf ein weiteres Problem in diesem Zusammenhang hat der TLfDI bei dieser Gelegenheit gleich hingewiesen. Das im Zusammenhang mit diesen Muttizetteln oftmals stattfindende Erheben und Speichern von Personalausweiskopien der Eltern ist rechtswidrig. Das Kopieren von Personalausweisen ist nur zulässig, wenn dieses Gesetz dies ausdrücklich für einen bestimmten Zweck erlaubt,

§ 14 Personalausweisgesetz. Für Muttizettel gib es eine solche Regelung nicht.

Muttizettel dürfen durch Verantwortliche i. S. d. Jugendschutzgesetzes bis zum Ende der Verjährungsfrist des möglichen Bußgeldverstoßes aufgehoben werden. Danach sind sie datenschutzgerecht zu vernichten. Personalausweiskopien sind in diesem Zusammenhang nicht zulässig.

2.7 Personalausweiskopie bei Bezug eines WG-Zimmers?

Der Beschwerdeführer hatte sich beklagt, dass eine Mitarbeiterin eines Maklerunternehmens für die Anwerbung eines WG-Zimmers die Kopie des Personalausweises forderte. Nachdem die Mieterin die Dame darauf hingewiesen hat, dass die Kopie des Personalausweises nur durch bestimmte öffentliche Stellen gefertigt werden dürfe, zeigte sich diese uneinsichtig. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist sodann an das Maklerunternehmen herangetreten und hat dieses darauf hingewiesen, dass für die Vermittlung von Wohnungen und in diesem Fall für die Vermittlung eines WG-Zimmers grundsätzlich keine Erforderlichkeit des Kopierens des Bundespersonalausweises besteht. Eine Rechtsgrundlage, die diese Art der Datenerhebung erlaubte, war in diesem Fall nicht gegeben. Die Unzulässigkeit der Anfertigung einer Kopie des gesamten Personalausweises ergibt sich insbesondere aus den §§ 14 ff. des Personalausweisgesetzes (PAuswG). Nach § 14 Nr. 2 PAuswG darf die Erhebung und Verwendung bestimmter personenbezogener Daten auf dem Ausweis oder mithilfe des Ausweises ausschließlich durch öffentliche und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20 PAuswG erfolgen. Die Vorlage eines Personalausweises dient vorrangig der Erfüllung der gesetzlich vorgeschriebenen Ausweispflichten im öffentlichen Bereich. Neben dem elektronischen Identitätsnachweis ist es nach dem PAuswG auch zulässig, den Personalausweis als Ausweis- und Legitimationspapier zu verwenden. Außer zum elektronischen Identitätsnachweis darf der Ausweis aber durch öffentliche und nicht-öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Nach den §§ 14 ff. PAuswG ist das Anfertigen von Kopien datenschutzrechtlich nicht zulässig, es sei denn, es ist durch eine

spezielle gesetzliche Ermächtigung erlaubt. Zum Nachweis der Identität eines Mieters ist es ausreichend, sich den Personalausweis vorlegen zu lassen und hierüber einen Vermerk zu machen, der allein die notwendigen Identitätsdaten, wie Name und Anschrift, enthält.

Der TLfDI hat das Maklerunternehmen aufgefordert, seine Mitarbeiterinnen und Mitarbeiter auf diese Rechtslage hinzuweisen und diese auch zu berücksichtigen. Eine Vorortkontrolle hat sich der TLfDI vorbehalten.

Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe der Ausweisdaten ist öffentlichen Stellen vorbehalten, § 14 PAuswG. Dabei ist darauf zu achten, dass das Kopieren des Personalausweises nur durch eine gesetzliche Regelung erlaubt werden kann und ansonsten grundsätzlich unzulässig ist. Eine Alternative zur Personalausweiskopie stellt das handschriftliche Aufzeichnen der für die Identitätsfeststellung notwenigen Daten dar. Diese sind nach § 18 PAuswG u. A. Name und Anschrift. Insbesondere die Seriennummer darf nicht aufgezeichnet und beim elektronischen Identitätsnachweis gemäß § 20 Abs. 3 PAuswG nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten möglich ist.

2.8 Online-Präsenz? Datenschutz nicht vergessen!

In einem kontrollierten Unternehmen, das im Einzelhandel tätig ist, wurde neben dem eigentlichen Ladengeschäft auch ein Online-Handel mit eigener Internetpräsenz betrieben. Die dafür benötigte Hardware wurde bei einem der vielen Hoster zusammen mit der Domain angemietet. Datenschutzrechtlich problematisch daran ist, dass jeder Kunde, der über diesen Shop etwas kauft, seine hierfür notwendigen Daten angeben muss. Diese darf zwar der Betreiber des Online-Shops erheben und speichern, allerdings werden in diesem Fall die Daten nicht durch den Betreiber des Shops gespeichert, sondern liegen, zumindest physisch, auf den Festplatten des Hosters. Damit speichert der Hoster personenbezogene Daten für den Betreiber des Online-Shops. Diese Art der Datenverarbeitung ist nur zulässig, soweit zwischen dem Hoster als Auftragnehmer und dem Online-Shop-Betreiber als Auftraggeber ein Auftragsdatenverarbeitungsverhältnis nach § 11 Bundesdatenschutzgesetz (BDSG) vereinbart

wird. Sobald also durch die Internetpräsenz personenbezogene Daten verarbeitet werden, muss ein solcher Vertrag geschlossen werden. Der Vertrag hat dem Schriftformerfordernis zu genügen. Dies setzt also voraus, dass der Vertrag in Papierform existiert und von beiden Parteien unterzeichnet wird. Eine E-Mail oder ein Fax genügt dieser Form nicht. Darüber hinaus muss der Gegenstand des Auftrags ausreichend bezeichnet, der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung der Daten, die Art der Daten und die Betroffenen müssen angegeben sein. Die zu regelnden notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG müssen ebenso enthalten sein wie ein dem Auftraggeber einzuräumendes Kontrollrecht. Auch eine Regelung, die den Auftragnehmer dem Weisungsrecht des Auftraggebers unterwirft und Ersteren verpflichtet, Verstöße gegen den Datenschutz seinem Auftraggeber zu melden, muss enthalten sein.

Einen solchen Vertrag hatte das Unternehmen mit seinem Hoster nicht geschlossen. Der Thüringer Landesbeauftragte forderte das Unternehmen auf, diesen rechtswidrigen Zustand zu beenden. Dies kann entweder durch Abschalten des Internetshops, den Umzug der Präsenz auf eigene Hardware oder am einfachsten durch Abschluss eines entsprechenden Vertrages über eine Auftragsdatenverarbeitung geschehen. Dem ist das Unternehmen nachgekommen und hat mit seinem Hoster einen Vertrag über die Auftragsdatenverarbeitung abgeschlossen.

Jedes Mal, wenn Datenverarbeitungsvorgänge ausgelagert werden und das übernehmende Unternehmen dabei weisungsgebunden bleiben soll, ist ein Vertrag über eine Auftragsdatenverarbeitung zu schließen. Dabei gibt es keine „Erheblichkeitsschwelle“. Es ist unerheblich, ob die Auslagerung nur vorübergehend, einmal oder regelmäßig erfolgt. Sobald Datenverarbeitungsvorgänge an Dritte gegeben werden, muss ein solcher Vertrag nach § 11 BDGS geschlossen werden.

2.9 Unsichere Post vom Sozialamt?

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie hatte erfahren, dass ein früherer Mitarbeiter eines privaten Zu-

stelldienstes äußerst unzuverlässig gewesen sei. Damit meinte sie, sich erklären zu können, weshalb sie Post vom Sozialamt in geöffneten Briefumschlägen erhalten hatte. Auf ihre Fragen an das Sozialamt hatte sie hierzu keine zufriedenstellenden Antworten erhalten.
Auf Nachfrage erklärte das Sozialamt, der genannte private Zustelldienst sei nicht von ihr mit der Zustellung von Behördenpost beauftragt. Das tatsächlich beauftragte Unternehmen versicherte der Stadtverwaltung, es habe an besagten Zustelldienst keinen Unterauftrag zur Zustellung der kommunalen Schreiben erteilt. Eine Zustellung von Schreiben des Sozialamts über den von der Beschwerdeführerin genannten privaten Zustelldienst war daher nicht erkennbar. Im Übrigen war dem Sozialamt keine weitere Beschwerde wegen geöffneter Post bekannt. Eine weitere Prüfung bei der Stadtverwaltung erübrigte sich daher.
Der genannte private Zustelldienst selbst unterliegt nicht der Kontrolle des TLfDI. Nach § 42 Abs. 3 Postgesetz (PostG) unterliegen Postzustelldienste der Kontrolle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Auf Wunsch der Beschwerdeführerin wurde die Beschwerde zuständigkeitshalber dorthin übersandt.

Für private Postzustelldienste ist nach § 42 Abs. 3 PostG die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig.

2.10 Datenschutzverstoß melden! – § 42a BDSG

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von einem Klinikum in privater Trägerschaft darüber informiert, dass ein meldepflichtiger Datenschutzverstoß passiert war. Dort hatte ein Patient in einem unbeobachteten Moment mit seinem Handy einen auf dem Schreibtisch eines Klinikmitarbeiters liegenden Brief fotografiert. Der Brief betraf einen Mitpatienten und enthielt zu diesem zweifelsohne äußerst sensible Angaben. Das Foto hatte der Fotograf sogleich an zwei weitere Mitpatienten geschickt.
Nach § 42a Bundesdatenschutzgesetz (BDSG) müssen nichtöffentliche Stellen die zuständige Datenschutzaufsichtsbehörde und alle Betroffenen unverzüglich über Datenschutzverstöße informieren. Die Verpflichtung besteht dann, wenn sie feststellen, dass bei ihnen

gespeicherte besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG oder personenbezogene Daten, die einem Berufsgeheimnis unterliegen, unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Dasselbe gilt für personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten (selbst wenn diesbezüglich nur der Verdacht vorliegt) beziehen und für personenbezogene Daten über Bank- oder Kreditkartenkonten. Darüber hinaus müssen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des Betroffenen drohen.
In der Meldung sind der Zeitpunkt und die konkreten Umstände der Verletzung des Schutzes personenbezogener Daten darzustellen. Darüber hinaus sind die technischen und organisatorischen Maßnahmen, die die meldepflichtige Stelle ergriffen hat oder ergreifen wird, aufzuführen. Hierzu zählen neben der Information des Betroffenen auch die Maßnahmen, die gegen denjenigen getroffen wurden, der die Datenschutzverletzung begangen hat. Ebenso sind die Gefahren für den Betroffenen und auch die Maßnahmen zur Minderung möglicher nachteiliger Auswirkungen für den Betroffenen aufzulisten. Kann man einen zu benachrichtigenden Betroffenen nur mit unverhältnismäßigem Aufwand ermitteln, bedarf es gegebenenfalls einer Information der Öffentlichkeit in geeigneter Form.
Im vorliegenden Fall war klar, dass man einen solchen Brief weder offen herumliegen lässt noch fotografieren und das angefertigte Foto weitergeben darf. Das Foto musste auf dem Handy des Datenschutzverletzers und selbstverständlich auch bei den beiden unbefugten Empfängern gelöscht werden. Dieser Personenkreis wurde durch die Klinik zur Löschung veranlasst. Weiterhin war sicherzustellen, dass zukünftig Vorfälle dieser Art nicht mehr passieren können. Hier hakte der TLfDI nochmals nach und fragte nach schriftlichen Festlegungen zum Umgang mit Patientenunterlagen. Im Ergebnis war festzustellen, dass die erforderlichen Maßnahmen umfassend dargelegt werden konnten. Die Klinikmitarbeiter waren auf die Wahrung des Datengeheimnisses verpflichtet; in einem Vortrag hatte der betriebliche Datenschutzbeauftragte den Vorfall für die Mitarbeiter nochmals ausgewertet. Darüber hinaus erhielten alle Mitarbeiter ein mahnendes Rundschreiben zum Vorfall und der Mitarbeiter, bei dem der Verstoß sich zugetragen hatte, wurde nochmals gesondert ermahnt. Damit war die Klinik ihren Verpflichtungen nachgekommen.

Der Pflicht zur Information des Betroffenen, war die Klinik ebenfalls nachgekommen.

Stellt eine nicht-öffentliche Stelle fest, dass bei ihr gespeicherte personenbezogene Daten der in § 42a Satz 1 BDSG genannten Kategorien unrechtmäßig übermittelt werden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte der schutzwürdigen Interesse des Betroffenen, hat sie dies unverzüglich der zuständigen Aufsichtsbehörde sowie dem Betroffenen mitzuteilen. Darüber hinaus sind geeignete Maßnahmen zu treffen, um zukünftig den Datenschutz sicherzustellen und andererseits die Beeinträchtigung des Betroffenen zu mildern.

2.11 Betrieblicher Datenschutzbeauftragter (bDSB): Kann das jeder?

Im Berichtszeitraum meldete sich ein Unternehmen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um einen Hinweis zu den gesetzlichen Anforderungen an einen betrieblichen Datenschutzbeauftragten. Weiterhin wollte das Unternehmen wissen, ob es zulässig sei, den EDV-Verantwortlichen des Unternehmens als betrieblichen Datenschutzbeauftragten zu bestellen. Die Bestellung des betrieblichen Datenschutzbeauftragten und die Anforderung an diesen sind in § 4f Bundesdatenschutzgesetz (BDSG) geregelt.
An einen betrieblichen Datenschutzbeauftragten werden zwar keine besonderen Voraussetzungen im Sinne einer besonderen Ausbildung gesetzt, jedoch verlangt das BDSG in § 4f Abs. 2 BDSG, dass dieser die erforderliche fachliche Eignung und Zuverlässigkeit besitzt. Hieraus lässt sich jedoch kein festes Anforderungsprofil bilden. Eine ausreichende Fachkunde kann nur dann angenommen werden, wenn die Person sowohl rechtliche als auch organisatorische und technische Kenntnisse in sich vereint. Welche Anforderungen im Einzelnen genügen, lässt sich deshalb, ganz im Sinne des § 4f Abs. 2 Satz 2 BDSG, nur sagen, wenn die spezifischen Umstände seiner Tätigkeit feststehen. Von unbestreitbarer Wichtigkeit jedoch sind ausreichend rechtliche Kenntnisse, um Hintergrundanforderungen und Ziele der datenschutzrelevanten rechtlichen Regelungen erkennen und so auch die Konsequenzen für die verantwortliche

Stelle ausmachen zu können. Summarische Kenntnisse reichen hierfür sicherlich nicht. Dies begründet sich darin, dass sich das Bundesdatenschutzgesetz durch eine ungewöhnlich hohe Anzahl an Generalklauseln und unbestimmten Rechtsbegriffen auszeichnet. Der Datenschutzbeauftragte muss daher in der Lage sein, eine datenschutzkonforme Interpretation selbst dann zu vertreten, wenn die vom Gesetzgeber geschaffenen Normen zumindest auf den ersten Blick keine klare Lösung aufzeigen.
Neben diesen juristischen Kenntnissen bedarf es auch organisatorischer und technischer Kenntnisse. Organisatorische Kenntnisse sind vonnöten, um Entscheidungsabläufe und Entscheidungsstrukturen innerhalb des betreuten Unternehmens nachvollziehen und durchdringen sowie die im Interesse einer datenschutzkonformen Verarbeitung erforderlichen Korrekturen anstreben zu können. Auf der technischen Seite muss der Datenschutzbeauftragte in der Lage sein, die technischen Hintergründe der einzelnen datenschutzrechtlich relevanten Verfahren zu durchdringen. Dies stellt eine unbedingte Voraussetzung für eine effektive Tätigkeit als betrieblicher Datenschutzbeauftragter dar.
Neben dieser fachlichen Eignung muss die Person mit einer ausreichenden Zuverlässigkeit ausgestattet sein. Hierbei sind objektive sowie subjektive Faktoren zu bedenken. Dabei beziehen sich subjektive Faktoren auf persönliche Eigenschaften, die objektiven auf mögliche Interessenkollisionen. An der notwendigen Zuverlässigkeit fehlt es beispielsweise, wenn die Person dafür bekannt ist, bereits gegen Datenschutzvorschriften verstoßen zu haben (subjektiver Faktor). Ebenfalls darf zwischen den sonstigen Aufgaben der Person im Betrieb und ihrer Aufgabe als betrieblicher Datenschutzbeauftragter kein Interessenkonflikt herrschen (objektiver Faktor).
Im Ergebnis konnte der TLfDI dem Unternehmen mitteilen, dass gegen die Bestellung des EDV-Verantwortlichen als betrieblichen Datenschutzbeauftragten bei Erfüllung der vorgenannten Voraussetzungen keinerlei Bedenken bestanden.

Nach § 4f Abs. 2 BDSG darf zum Beauftragten für den Datenschutz nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Die Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und der Schutzbedürftigkeit der verarbeiteten personenbezogenen Daten. Je

sensibler die Daten, desto größer sind die Anforderungen an die Fachkunde.

2.12 Notwendigkeit eines Datenschutzbeauftragten nach BDSG bei verschiedenen Erscheinungsformen des Maklerberufes

Im Berichtszeitraum wandte sich ein externer Datenschutzbeauftragter mit der Bitte um Hinweise zur Erforderlichkeit eines Datenschutzbeauftragten bei verschiedenen Erscheinungsformen des Versicherungsmaklerberufes an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Folgende Erscheinungsformen des Versicherungsmaklerberufes kommen bei einem Versicherungsmaklerunternehmen in Betracht: 1. Festangestellter Mitarbeiter im Innen- und/oder Außendienst; 2. Handelsvertreter als selbstständiger Gewerbetreibender i. S. d. § 84 Handelsgesetzbuch (HGB) – „Einfirmenvertreter“, der damit beauftragt ist, nur für ein Versicherungsmaklerunternehmen Geschäfte (Verträge) zu vermitteln und/oder in deren Namen abzuschließen; 3. Freier Mitarbeiter der für mehrere Versicherungsunternehmen selbstständig arbeitet bzw. das Vermittlungsgeschäft betreibt – „Mehrfachfirmenvertreter“; 4. Versicherungsmakler nach § 93 HGB, dieser ist nicht vertraglich an eine Versicherungsgesellschaft gebunden, sondern steht als „treuhänderähnlicher Sachwalter“ der Interessen des Versicherungsnehmers auf dessen Seite.
Zunächst musste der TLfDI für die Prüfung der Erforderlichkeit eines Datenschutzbeauftragten die vorgenannten Erscheinungsformen des einzelnen Versicherungsmaklerberufes unterscheiden. Konkret, ob dieser eine eigene verantwortliche Stelle darstellte oder als Teil einer verantwortlichen Stelle tätig war. Nach § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) ist jede Person oder Stelle verantwortliche Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder diese durch einen anderen im Auftrag vornehmen lässt. Ein Festangestellter im Innen- und/oder Außendienst bei einem Versicherungsmaklerunternehmen stellt jedenfalls keine eigene verantwortliche Stelle im Sinne des BDSG dar. Dagegen stellen der Handelsvertreter nach § 84 HGB sowie auch der Handelsmakler nach § 93 HGB für sich in der Regel selbstständige Tätigkeiten dar. Daher sind diese als eigene verantwortliche Stelle im Sinne des BDSG zu betrachten. Unbeachtlich ist dabei, ob diese

Tätigkeit jeweils für einen oder mehrere Unternehmer (§ 84 HGB) oder Personen (§ 93 HGB) durchgeführt wird.
Diese verantwortlichen Stellen müssen nach § 4f Abs. 1 BDSG einen Beauftragten für den Datenschutz (bDSB) bestellen, wenn sie unabhängig von der Zahl der Beschäftigten als verantwortliche Stelle personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (z. B. Adresshandel, Auskunfteien etc.) oder der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung erheben, verarbeiten oder nutzen, § 4f Abs. 1 Satz 6 BDSG. Darüber hinaus verpflichtet das BDSG Unternehmen zur Bestellung eines betrieblichen Datenschutzbeauftragten unabhängig von der Zahl der Beschäftigten, wenn sie als verantwortliche Stelle automatisierte Datenverarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, § 4f Abs. 1 Satz 5 BDSG.
Sind diese besonderen Voraussetzungen nicht gegeben, hängt die Pflicht zur Berufung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich von der Zahl der Personen ab, die mit der Datenverarbeitung beschäftigt sind. Ein Datenschutzbeauftragter muss bestellt werden, wenn in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten oder in der Regel mindestens zwanzig Personen mit der Verarbeitung, Nutzung oder Erhebung personenbezogener Daten auf andere Weise (manuelle Verarbeitung) beschäftigt sind. Maßgeblich ist nicht die Anzahl der Arbeitnehmer, sondern die der im Unternehmen tätigen "Personen" (d. h. auch freie Mitarbeiter, Auszubildende und Geschäftsführer).
Der betriebliche DSB ist innerhalb einer Frist von einem Monat nach Aufnahme der Tätigkeit der nicht-öffentlichen Stelle zu bestellen. Wird der Datenschutzbeauftragte vorsätzlich oder fahrlässig nicht oder nicht rechtzeitig bestellt, so stellt dies eine Ordnungswidrigkeit dar, die mit einer Geldbuße geahndet werden kann.

Nicht-öffentliche Stellen wie juristische Personen (z. B. Aktiengesellschaften, GmbHs), Personengesellschaften (z. B. Gesellschaften des bürgerlichen Rechts), auch nicht rechtsfähige Vereinigungen (z. B. Gewerkschaften, politische Parteien) ebenso wie natürliche Personen (z. B. Ärzte, Rechtsanwälte, Architekten) können nach dem BDSG grundsätzlich verpflichtet sein, Datenschutzbeauftragte zu bestellen, vergleiche § 4f BDSG.

2.13 Wann braucht man einen eigenen betrieblichen Datenschutzbeauftragten (bDSB)?

Im Berichtszeitraum erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gleich mehrere Fragen eines Mitarbeiters zum betrieblichen Datenschutzbeauftragten. Ein Mitarbeiter hatte bereits erfolgreich ein Seminar zum bDSB absolviert und sollte nun der bDSB für eine Holding mit deren fünf Tochtergesellschaften werden. Vornehmlich ging es dem Mitarbeiter darum, ob nur ein betrieblicher Datenschutzbeauftragter für alle Tochtergesellschaften und für die Holding selbst bestellt werden muss und ob diese Aufgabe durch ein und dieselbe Person ausgeführt werden kann. Weiterhin fragte der Mitarbeiter den TLfDI, ob eine einzelne Person nach erfolgreichem Abschluss eines Seminars zum bDSB auch ohne ausdrückliche Bestellung vom Unternehmen zum betrieblichen Datenschutzbeauftragten diese Funktion ausüben könnte.
Nach Überprüfung der Sach- und Rechtslage antwortete der TLfDI dem Mitarbeiter, dass nach § 4f Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich zu bestellen haben. Mit der Schriftform unterstreicht das Gesetz die Bedeutung, die es den Aufgaben des Beauftragten beimisst. Schon der Art und Weise der Bestellung muss deshalb klar zu entnehmen sein, dass es sich um eine besondere Position mit einem eigenen, gesetzlich definierten Aufgabenkreis handelt. § 4f Abs. 1 Satz 1 BDSG verlangt eine von beiden Seiten unterschriebene Urkunde im Sinne des § 126 Bürgerlichen Gesetzbuches (BGB) und nicht etwa nur eine schriftliche Mitteilung. Auf die rechtliche Beziehung zwischen der verantwortlichen Stelle und dem Beauftragten kommt es dabei nicht an (Simitis, BDSG, 8. Auflage, § 4f Rn. 56f.)
Weiterhin teilte der TLfDI dem Mitarbeiter mit, dass grundsätzlich in einer Holding mit Tochtergesellschaften für jede einzelne juristische Person, d. h. für jedes Unternehmen, ein Beauftragter für den Datenschutz, soweit die Voraussetzungen hierfür gegeben sind, bestellt werden muss (vergleiche Simitis, BDSG, 8. Auflage, § 4f. Rn. 35). Das BDSG hat sich hier für einen eindeutig formalen Bezugspunkt entschieden. Das heißt, noch so enge, wirtschaftlich begründete und organisatorisch abgesicherte Beziehungen zwischen den einzelnen Unternehmen müssen hinter der rechtlichen Selbst-

ständigkeit zurückstehen. Von dieser ist abhängig, ob ein Unternehmen eine eigene verantwortliche Stelle im Sinne des BDSG darstellt. Wenn diese dann auch nach § 4f BDSG verpflichtet ist, einen bDSB zu bestellen, dann hat sie diese Pflicht zu erfüllen. Vorliegend würde daher hier ein Beauftragter allein für die Holding, die ja aus verschiedenen verantwortlichen Stellen besteht, nicht genügen, sofern die Tochtergesellschaften nicht wegen der geringen Anzahl der Beschäftigten oder der Organisation der Datenverarbeitung unter die Ausnahme des § 4f Abs. 1 BDSG fallen würden. Denn nach § 4f Abs. 1 Satz 1 i. V. m. Satz 4 BDSG sind nicht-öffentliche Stellen zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Maßgeblich ist, dass die jeweils betroffenen Personen Aufgaben erfüllen, die mit der Verarbeitung personenbezogener Daten zusammenhängen. Voll- und Teilzeitkräfte sind infolgedessen gleichermaßen einzubeziehen. Genauso wenig spielen die im Einzelnen wahrgenommenen Aufgaben eine Rolle. Das Tatbestandsmerkmal „ständig“ im Sinne der vorgenannten Vorschrift soll ausschließen, dass auch solche Personen in den maßgeblichen Personenkreis mit einbezogen werden, die nur als Urlaubs- oder Krankheitsvertretung personenbezogene Daten automatisiert verarbeiten. Wer also nur gelegentlich oder im Rahmen ganz anderer Funktionen mit der Verarbeitung zu tun hat, zählt nicht zu den nach § 4f Abs. 1 Satz 4 BDSG zu berücksichtigenden Personen. Hingegen genügt es für die Anwendung des § 4f Abs. 1 Satz 4 BDSG, wenn das Arbeitsprogramm der jeweils in Betracht kommenden Beschäftigten einen festen Posten aufweist, der es erlaubt, sie der Verarbeitung personenbezogener Daten zuzuordnen (vergleiche Simitis, 8. Auflage, § 4f Rn. 12 ff.).
Für jede Tochtergesellschaft und für die Holding kann aber ein und dieselbe Person zum betrieblichen Datenschutzbeauftragten bestellt werden (vergleiche Simitis BDSG, 8. Auflage, § 4f Rn. 36 f.). Dabei ist aber zu beachten, dass dieser, wie bereits ausgeführt, für jedes einzelne Unternehmen selbst schriftlich bestellt werden muss.
Der TLfDI teilte dem Mitarbeiter seine rechtliche Auffassung mit. Weitere Information zum bDSB sind auf der Homepage des TLfDI unter https://www.tlfdi.de/imperia/md/content/dat

enschutz/themen/unterneunte/checkliste_bdsb.pdf zu finden.

Soweit ein Unternehmen mehrere, rechtliche selbstständige Einheiten umfasst, ist jede von ihnen verpflichtet, einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen, vergleiche § 4f Abs. 1 BDSG. Die Bestellung zum betrieblichen Datenschutzbeauftragten muss schriftlich erfolgen. § 4f Abs. 1 Satz 1 BDSG verlangt sowohl vom Unternehmen als auch vom zukünftigen betrieblichen Datenschutzbeauftragten eine unterschriebene Urkunde im Sinne des § 126 BGB und nicht nur eine mündliche oder schriftliche Mitteilung.

2.14 Datenschutzbeauftragter nur mit Qualifikation

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die anonyme Beschwerde einer Krankenschwester, die aus Furcht, ihren Arbeitsplatz zu verlieren, weder ihren Namen noch den konkreten Vorfall benennen wollte, um den es ihr ging. Es gäbe in dem Krankenhaus, in dem sie beschäftigt sei, einen externen Datenschutzbeauftragten. Er habe wenig Zeit für Anfragen, Betroffene mit Datenschutzfragen würden abgewiesen und irgendwie habe sie das Gefühl, er wisse gar nicht richtig, worum es gehe. Ihre Frage war, ob denn jeder Datenschutzbeauftragter werden könne oder man dazu eine Ausbildung brauche. Sie wollte auch wissen, wer die Qualifikation des Datenschutzbeauftragten überprüft und bat den TLfDI tätig zu werden.
Der TLfDI wandte sich an das Krankenhaus, schilderte die erhobenen Vorwürfe und teilte mit, dass für die Berufung als Datenschutzbeauftragter zwar keine spezielle Berufsausbildung erforderlich sei, nach § 4f Abs. 2 Satz 1 Bundesdatenschutzgesetz zum Beauftragten für den Datenschutz aber nur bestellt werden dürfe, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Aufgrund der sich schnell verändernden Medienlandschaft ist es auch unerlässlich, dass sich Datenschutzbeauftragte regelmäßig fortbilden. Das Krankenhaus wurde gebeten, zu den erhobenen Vorwürfen Stellung zu beziehen und vor allem auch mitzuteilen, über welche Qualifikation sein Datenschutzbeauftragter verfügt und wie oft er an Weiterbildungen teilnimmt.
Das Krankenhaus überdachte daraufhin die vorgenommene Bestellung seines Datenschutzbeauftragten und bestellte eine andere Per-

son mit sofortiger Wirkung. Diese Person verfügte nach den eingereichten Unterlagen über eine umfassende Ausbildung in Datenschutzfragen und bildete sich regelmäßig fort. Damit war die Angelegenheit für den TLfDI erledigt.

Zwar bedarf es keiner speziellen Berufsausbildung, um zum Datenschutzbeauftragten bestellt zu werden. Die verantwortliche Stelle muss aber eine Person mit dieser Funktion betreuen, die die zur Erfüllung der Aufgaben des Datenschutzbeauftragten erforderliche Fachkunde und Zuverlässigkeit besitzt.

2.15 Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten

Aufgrund einer anonymen Beschwerde erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis, dass ein Unternehmen keinen betrieblichen Datenschutzbeauftragten (bDSB) bestellt hatte, obwohl, so wurde behauptet, dieses hierzu verpflichtet war.
Das daraufhin an das Unternehmen gerichtete schriftliche Auskunftsverlangen des TLfDI nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) bestätigte dies. In dem Unternehmen waren vier Personen vornehmlich mit der automatisierten Datenverarbeitung beschäftigt. Darüber hinaus waren bei dem Unternehmen zehn Abteilungsleiter angestellt, deren Aufgabe neben vielen anderen es war, Korrekturen direkt im Zeiterfassungssystem vorzunehmen und damit personenbezogene Daten automatisiert zu verarbeiten. Das Unternehmen war der Ansicht, dass die Korrekturtätigkeit der Abteilungsleiter noch nicht die Bestellung eines Datenschutzbeauftragten erforderlich machte, weil es sich dabei nur um eine Aufgabe unter vielen, und damit nicht um eine ständige handelte.
Nach § 4f Abs. 1 Satz 1 i. V. m. Satz 4 BDSG sind nicht-öffentliche Stellen zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Maßgeblich ist danach, dass die jeweils betroffenen Personen Aufgaben erfüllen, die mit der Verarbeitung personenbezogener Daten zusammenhängen. Voll- und Teilzeitkräfte sind infolgedessen gleichermaßen einzubeziehen. Genauso wenig spielen die im Einzelnen wahrgenommenen Aufgaben eine Rolle. Das Tatbestandsmerk-

mal „ständig“ im Sinne der vorgenannten Vorschrift soll ausschließen, dass auch solche Personen in den maßgeblichen Personenkreis mit einbezogen werden, die nur als Urlaubs- oder Krankheitsvertretung personenbezogene Daten automatisiert verarbeiten. Wer also nur gelegentlich oder im Rahmen ganz anderer Funktionen, wie etwa die Mitarbeiter der Revisionsabteilung oder die Wartungstechniker, mit der Verarbeitung zu tun hat, zählt nicht zu den nach § 4f Abs. 1 Satz 4 BDSG zu berücksichtigenden Personen. Hingegen genügt es für die Anwendung des § 4f Abs. 1 Satz 4 BDSG, wenn das Arbeitsprogramm der jeweils in Betracht kommenden Beschäftigten einen festen Posten aufweist, der es erlaubt, sie der Verarbeitung personenbezogener Daten zuzuordnen (vergleiche Simitis, 8. Auflage, § 4f Randnummer 12 ff.).
In der Konsequenz ergab sich für den TLfDI, dass in dem Unternehmen in der Regel 14 Personen ständig mit der automatisierten Datenverarbeitung beschäftigt waren. Daraus folgte die Pflicht zur Bestellung eines bDSG nach § 4f Abs. 1 Satz 1 i. V. m. Satz 4 BDSG in dem Unternehmen. Zur Bestellung eines solchen bDSG war das Unternehmen einen Monat nach Aufnahme des Geschäftsbetriebes verpflichtet, § 4f Abs.1 Satz 2 BDSG. Die Aufnahme des Geschäftsbetriebes erfolgte bereits im Jahr 2013. Deshalb forderte der TLfDI das Unternehmen auf, einen betrieblichen Datenschutzbeauftragten zu bestellen, der auch den Voraussetzungen des § 4f Abs. 2 BDSG entspricht. Zu den Voraussetzungen hat der TLfDI bereits ausführlich in diesem Tätigkeitsbericht informiert, es wird daher auf Nummer 2.11 verwiesen.
Letztendlich konnte der TLfDI das Verwaltungsverfahren beenden. Denn das Unternehmen hat einen Mitarbeiter zum betrieblichen Datenschutzbeauftragten bestellt und dies dem TLfDI gegenüber nachgewiesen.

Nach § 4f Abs. 1 Satz 1 i. V. m. Satz 4 BDSG sind nicht-öffentliche Stellen zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Entscheidend ist ausschließlich die Anzahl der bei der Verarbeitung beschäftigten Personen und nicht die Arbeitnehmereigenschaft. Voll- und Teilzeitbeschäftigte sind infolgedessen gleichermaßen einzubeziehen.

2.16 Betrieblicher Datenschutzbeauftragter bei automatischer Verarbeitung politischer Mitgliedsdaten

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Rechtsanwalts hinsichtlich der Notwendigkeit der Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) in einem Landesverband einer politischen Partei. Der Landesverband verarbeitete die Daten der Mitglieder automatisiert.
Zunächst haben nicht-öffentliche Stellen gemäß § 4f Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG), die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich zu bestellen. Dazu sind nicht-öffentliche Stellen nach Satz 2 spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Diese Pflicht entfällt nur dann, wenn es sich um eine verantwortliche Stelle handelt, die maximal neun Personen mit der automatisierten Datenverarbeitung beschäftigt. Werden Daten nicht automatisiert verarbeitet, was heute kaum mehr vorkommt, ist ab 20 Personen, die mit dieser Datenverarbeitung beschäftigt sind, ebenfalls ein betrieblicher Datenschutzbeauftragter (bDSB) zu bestellen. (vergleiche dazu § 4f Abs. 1 Satz 3 und 4 BDSG). Unterfällt jedoch die Datenverarbeitung der Pflicht einer Vorabkontrolle, ist in jedem Fall und unabhängig von den o. g. Grenzen ein bDSB zu bestellen, § 4f Abs. 1 Satz 6 BDSG. Nach § 4d Abs. 5 Satz 1 BDSG unterliegen automatisierte Verarbeitungen der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle), soweit sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dies ist insbesondere dann der Fall, wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden, § 4d Abs. 5 Satz 2 Nr. 1 BDSG. Besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Aus einer bestimmten Parteizugehörigkeit lässt sich das Vertreten von bestimmten politischen Meinungen ableiten. Die Zugehörigkeit zu einer politischen Partei beinhaltet dabei bereits ein über eine politische Meinungsäußerung hinausgehendes Mehr (Simitis, Kommentar zum Bundesdatenschutzgesetz, 8. Auflage, § 3 Rn. 261). Das BDSG gibt hierbei zu erkennen, dass die Vorschriften zur Verarbeitung besonderer Arten personenbezogener

Daten nicht erst zum Zuge kommen sollen, wenn jemand einer politischen Partei angehört, sondern bereits dann, wenn politische Meinungen in Datensätzen erkennbar werden. Daher ist die Parteizugehörigkeit, auch ohne explizite Nennung im § 3 Abs. 9 BDSG unter die besonderen Arten personenbezogener Daten zu subsumieren. Der TLfDI konnte im Ergebnis feststellen, dass im vorliegenden Fall die Mitgliedsdaten zum Landesverband einer politischen Partei besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG waren.
Da es sich also bei Parteizugehörigkeit um eine besondere Art eines personenbezogenen Datums handelt, war nach § 4d Abs. 5 Satz 2 Ziffer 1 BDSG eine Vorabkontrolle durchzuführen, mit der unmittelbaren Folge der Bestellpflicht eines betrieblichen Datenschutzbeauftragten nach § 4f Abs. 1 Satz 6 BDSG. Der Anfragende wurde vom TLfDI hierüber informiert.

Nach § 4d Abs. 5 Satz 2 Nr. 1 ist eine Vorabkontrolle insbesondere durchzuführen, wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden. Bei der Parteizugehörigkeit handelt es sich um eine besondere Art personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG. Die durchzuführende Vorabkontrolle führt zur Bestellpflicht eines betrieblichen Datenschutzbeauftragten nach § 4f Abs. 1 Satz 6 BDSG.

2.17 Betrieblicher Datenschutzbeauftragter = EDV-Administrator?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage eines Thüringer Unternehmens, mit der Bitte um Mitteilung, ob ein Vertreter des Leiters der Elektronischen Datenverarbeitung (EDV) als interner betrieblicher Datenschutzbeauftragter (bDSB) bestellt werden könne oder ob diese Bestellung zu einem Interessenkonflikt führe. Bei dem für die Bestellung als internen bDSB geplanten Mitarbeiter handelte es sich um den ehemaligen Leiter der EDV. Dieser sollte auch weiterhin administrative Zugriffsrechte auf die verschiedenen IT-Systeme haben und aktiv Systemkonfigurationen vornehmen können.
Das Bundesdatenschutzgesetz (BDSG) hat in § 4f Abs. 2 Satz 1 BDSG die Bestellung des Beauftragten an zwei Qualifikationsmerkmale geknüpft: Fachkunde und Zuverlässigkeit. Bei der

Zuverlässigkeit sind subjektive genauso wie objektive Faktoren zu bedenken. Die subjektiven Faktoren beziehen sich auf persönliche Eigenschaften der Person an sich, während die objektiven Faktoren sich auf mögliche Interessenkollisionen zwischen den Aufgaben als betrieblicher Datenschutzbeauftragter und eventuellen sonstigen Aufgaben beziehen. Eine Bestellung zum betrieblichen Datenschutzbeauftragten kann daher nur erfolgen, wenn die erforderlichen persönlichen Eigenschaften gegeben sind und keine Interessenkollisionen vorliegen, die sich nachteilig auf die Tätigkeit des Beauftragten auswirken können.
Vorliegend stellte der TLfDI fest, dass man nicht pauschal davon ausgehen könne, dass ein Vertreter des Leiters der EDV nicht zuverlässig im Sinne des § 4f Abs. 2 Satz 1 BDSG sei. Jedoch sprach hier einiges dafür, denn jedenfalls im Vertretungsfall würde es zwangsweise zu Interessenkollisionen führen. Da es sich bei dem als bDSB geplanten Mitarbeiter um den ehemaligen Leiter der EDV in dem Unternehmen handelte, war hier für den TLfDI der Interessenkonflikt bereits darin zu sehen, dass der Mitarbeiter seine in der Vergangenheit getroffenen und umgesetzten Entscheidungen zu prüfen hätte. Die Zuverlässigkeit im Sinne des § 4f Abs. 2 Satz 1 ist dabei nicht mehr sichergestellt.
Im Ergebnis teilte der TLfDI daher dem Thüringer Unternehmen mit, dass eine Bestellung des ehemaligen Leiters der EDV zum bDSG wegen einer Interessenkollision nicht wirksam wäre.

Nach § 4f Abs. 2 Satz 1 BDSG darf zum Beauftragten für den Datenschutz nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Die Zuverlässigkeit ist an subjektive und objektive Faktoren des Beauftragten geknüpft. Die subjektiven beziehen sich auf persönliche Eigenschaften, die objektiven auf mögliche Interessenkollisionen. Zumindest darf ein Administrator nicht zugleich Datenschutzbeauftragter sein, da er sonst seine eigenen Maßnahmen zu kontrollieren hätte.

2.18 Systemadministration und Passwortsicherheit – ohne verbindliche Regelungen kein Schutz

Ein modernes Unternehmen kann auf eine funktionierende interne IT-Infrastruktur nicht verzichten. Um diese zu verwalten, ist ein System-Administrator notwendig. Doch dieser kümmert sich nicht

nur um die Verwaltung der Systeme, sondern ist auch für den sicheren Betrieb dieser Systeme verantwortlich.
Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage, ob es ausreichend sei, wenn die Administration der Rechner durch einen IT-Mitarbeiter der Geschäftsstelle durchgeführt wird. Darüber hinaus verwaltete dieser IT-Mitarbeiter die Website sowie die Mailadressen inklusive der entsprechenden Kennwörter. Daneben waren diese Kennwörter noch beim betrieblichen Datenschutzbeauftragten (bDSB), welcher nicht mit dem o. g. IT-Mitarbeiter identisch ist, hinterlegt.
Der TLfDI hatte aufgrund der personellen Trennung der Rollen des Datenschutzbeauftragen und des IT-Administrators gegen die Regelung, dass die Kennwörter beim bDSB hinterlegt werden, nur insoweit nichts einzuwenden, als dies für zentrale System-Administrations-Passwörter gilt und wenn die Hinterlegung der Sicherstellung des ordnungsgemäßen Arbeitsbetriebs bei Krankheits-, Urlaubs- oder anderen gleichartigen Fällen dient. Weiterhin ist sicherzustellen, dass zentrale System-Administrations-Passwörter verschlossen in einem Schrank, Tresor bzw. dort wiederum in einem ebenfalls verschlossenen Briefumschlag abgelegt werden. Unbefugte dürfen auf diese Kennwörter keinen Zugriff haben. Der TLfDI forderte zudem, dass das Vorgenannte in einer Dienstanweisung zu regeln ist. In dieser ist mit Blick auf die Passwortsicherheit außerdem festzulegen, wer unter welchen Voraussetzungen auf die zentralen System-Administrations-Passwörter zugreifen kann.
Neben den genannten zentralen System-Administrations-Passwörtern hat jeder Administrator ausschließlich mit seiner eigenen Administrationskennung zu arbeiten. Letztere sowie die Mitarbeiter-Passwörter dürfen grundsätzlich nur dem jeweiligen Mitarbeiter bekannt sein. Solche Passwörter dürfen daher auch grundsätzlich nicht bei Dritten, also auch bei den jeweiligen Datenschutzbeauftragten, in einem Umschlag hinterlegt werden. Zudem sind Gruppenkennungen zu vermeiden.
Weiterhin sollte bei der Passwortwahl die Maßnahme M 2.11 der IT-Grundschutz-Kataloge des Bundesamts für Informationssicherheit (BSI) umgesetzt werden.
Auf Nachfrage teilte der TLfDI mit, dass es nicht notwendig sei, die Administration der PCs von einem externen Dritten vornehmen zu lassen.

Zentrale System-Administrations-Passwörter dürfen nur in begründeten Fällen beim betrieblichen Datenschutzbeauftragten hinterlegt werden. Diese sind dann in einem verschlossenen Umschlag in einem Safe zu hinterlegen. Mitarbeiter-Passwörter einschließlich individueller Administrations-Passwörter dürfen Dritten nicht zugänglich sein.

2.19 Datenschutz-Informationspflichten bei Datenpannen nach § 42a BDSG

Ob Datenleck, Datenpanne oder Datendiebstahl: Oft stehen dabei die betroffenen Stellen vor der unangenehmen Frage, ob solche Zwischenfälle der Aufsichtsbehörde gemeldet werden müssen. Das Bundesdatenschutzgesetz (BDSG) hält hierfür eine eindeutige Regelung parat.
Es hängt im Wesentlichen von den betroffenen personenbezogenen Daten ab. Eine Meldepflicht besteht nur, wenn es sich bei den betroffenen Daten um

1 besondere Arten personenbezogener Daten,
2 personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3 personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4 personenbezogene Daten zu Bank- oder Kreditkartenkonten

handelt.
Werden solche Arten von Daten unrechtmäßig übermittelt oder gelangen diese auf sonstige Weise Dritten unrechtmäßig zur Kenntnis, sind nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen nach § 42a BDSG dazu verpflichtet, sowohl die Aufsichtsbehörde als auch die Betroffenen zu benachrichtigen. Diese Pflicht greift nur, wenn für die Rechte oder schutzwürdigen Interessen der Betroffenen schwerwiegende Beeinträchtigungen drohen. Dabei kommt es darauf an, welche Auswirkungen die unrechtmäßige Kenntniserlangung durch Dritte für die Betroffenen haben kann. Die betroffene Stelle muss eine Prognoseentscheidung treffen, d. h. sie muss mögliche Folgen nach Lage der Dinge identifizieren und diese anhand der Belastung für die Betroffenen und der Wahrscheinlichkeit, dass die Belastung eintritt, bewerten. Für den Fall, dass die

betroffene Stelle zu dem Ergebnis kommt, dass keine schwerwiegenden Beeinträchtigungen drohen und sie die Benachrichtigung der Betroffenen folglich unterlässt, muss sie gegenüber der Aufsichtsbehörde nachweisen können, warum sie zu diesem Ergebnis gekommen ist. Bei den o. g. Datenkategorien müssen schon gute Gründe gegen eine solche schwerwiegende Beeinträchtigung sprechen.
Die Daten müssen bei der betroffenen Stelle gespeichert (gewesen) sein, d. h. wenn die Daten beim Betroffenen selbst abhandenkommen (z. B. PIN und TAN-Nummer beim Onlinebanking), ist § 42a BDSG nicht einschlägig. Dagegen kann eine Meldung nach § 42a BDSG in Betracht kommen, wenn Daten unbefugt aus einem IT-System abgerufen werden, indem Passwörter, Zugangscodes, Skriptinformationen etc. verwendet werden, die der Angreifer sich beim Betroffenen oder auf anderem Wege (z. B. über Social Engineering) beschafft hat.
Letztlich soll nicht unerwähnt bleiben, dass, wer der gesetzlichen Verpflichtung nicht oder nicht rechtzeitig nachkommt, mit einem Bußgeld von bis zu 300.000 Euro gemäß § 43 Abs. 2 Nr. 7, Abs. 3 BDSG rechnen kann. Es steht also einiges auf dem Spiel.
Wegen der geringen Anzahl an Eingängen von Meldungen vorgenannter Datenpannen im Berichtszeitraum hat sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) der Eindruck eingestellt, dass die Thüringer Unternehmen vorgenannte Zwischenfälle nicht durchweg melden. Dies hat der TLfDI bereits zum Anlass genommen, die Unternehmen über die Industrie- und Handelskammern und deren Mitgliederzeitschriften über diese Informationspflicht zu belehren.
Um den Unternehmen das Erfüllen dieser Pflicht noch einfacher zu gestalten, hat der TLfDI eine Checkliste entwickelt, die möglichst viele Fragen zu § 42a BDSG abdeckt. Die Fragen und Antworten sollen dabei den Unternehmen helfen, die mitteilungspflichtigen Sachverhalte zu identifizieren und die entstehenden Handlungspflichten zu erkennen bzw. umzusetzen. Die Checkliste ust im Internet auf der Homepage des TLfDI unter https://www.tlfdi.de/imperia/md/content/datenschutz/mustervordrucke/checkliste_42bdsgneu.pdf veröffentlicht.

§ 42a BDSG verpflichtet nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen, den TLfDI und die Betroffenen unverzüglich darüber zu benachrichtigen, wenn entsprechend sensible Daten (z. B. Gesundheitsdaten, Konto- und Kreditkarteninformationen) Dritten unrechtmäßig zur Kenntnis gelangt sind (z. B. durch einen Hackerangriff oder beispielsweise den Diebstahl eines unverschlüsselten Laptops). Bei entsprechend schwerwiegenden Verstößen drohen nach § 43 Abs. 2 BDSG Bußgelder von bis zu 300.000 Euro. Wann dies im Einzelnen der Fall ist und welche Konsequenzen daraus folgen, soll mithilfe einer vom TLfDI entwickelten Checkliste näher erläutert werden.

2.20 Es kommt auf den Auftraggeber an, um die Zuständigkeit zu beurteilen

Ein Unternehmen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Beratung. Hintergrund war, dass das Unternehmen, das seinen Sitz in Thüringen hatte, von einem bundesweit auftretenden Unternehmen mit Sitz in Baden-Württemberg einen Vertrag zur Auftragsdatenverarbeitung erhalten hatte. Gegenstand des Vertrages war die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag des Auftraggebers zum Zweck der Lieferung von vertraglichen Leistungen (Warenlieferung), der Werbung, der Abwicklung des Zahlungsverkehrs und des Controllings.
In diesem Fall sah der TLfDI keine Möglichkeit, das Thüringer Unternehmen zu beraten. Zwar ist er nach § 42 Thüringer Datenschutzgesetz i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Gemäß § 38 Abs. 1 Satz 2 BDSG berät und unterstützt er die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Hier ist aber das Wesen der Auftragsdatenverarbeitung zu beachten, das darin liegt, dass der Auftraggeber für die Datenverarbeitung verantwortlich bleibt, § 11 BDSG. Er muss bestimmen, wie die Datenverarbeitung beim Auftragnehmer abzulaufen hat und welche Maßnahmen im Einzelnen zu treffen sind. Im konkreten Fall bedeutet dies, dass das auftraggebende Unternehmen mit Sitz in Baden-Württemberg den Inhalt des Auftragsdatenverarbeitungsvertrages bestimmen muss. Zuständig für die datenschutzrechtliche Überprüfung des Vertragsinhaltes anhand der von § 11 BDSG aufge-

stellten Maßstäbe ist der für das auftraggebende Unternehmen zuständige Landesbeauftragte für Datenschutz. Das Thüringer Unternehmen wurde daher gebeten, sich dorthin zu wenden.

Das Wesen der Auftragsdatenverarbeitung besteht darin, dass der Auftraggeber für die Datenverarbeitung verantwortlich bleibt, § 11 BDSG. Zuständig für die datenschutzrechtliche Prüfung eines Vertrages zur Auftragsdatenverarbeitung ist immer die Aufsichtsbehörde, die für das auftraggebende Unternehmen zuständig ist.

2.21 Man kann kein Gras darüber wachsen lassen! Veröffentlichung von Namen ehemaliger Mitarbeiter des MfS

Ein Sohn wendet sich für seinen Vater an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Beim Recherchieren mit dem Vor- und Nachnamen seines Vaters gelangte er auf eine Webseite eines Vereins, die eine Liste von ehemaligen Mitarbeitern des Ministeriums für Staatssicherheit (MfS) veröffentlicht hat. Auch der Name des Vaters stand auf der Liste. Er fragte den TLfDI nach der rechtlichen Grundlage, auf die sich der betreffende Verein berufen kann. Die Anfrage bei dem Verein sowie die Auswertung weiterer Veröffentlichungen im Internet haben Folgendes ergeben: Die angesprochene Liste ist im Rahmen eines Forschungsprojektes erarbeitet worden. Die Daten und Informationen sind das Ergebnis mehrerer Forschungsanträge bei der Behörde des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) sowie von Recherchen aus Akteneinsichten des Vereins. Die rechtliche Grundlage für die angesprochenen Veröffentlichungen stellt das Stasi-Unterlagen-Gesetz (StUG) dar. Der Verein berief sich weiterhin auf ein Urteil vom Oberlandesgericht München vom 14. Dezember 2010, Az.: 18 U 3097/09, welches die Klage eines früheren inoffiziellen Mitarbeiters (IMB) für Staatssicherheit in der DDR (MfS) gegen den Verantwortlichen der Internetseite abwies. Der ehemalige IMB wollte seine Ansprüche auf medienrechtliche Löschung und Unterlassung gelten machen. Das Urteil bezieht sich u. a. auf § 32 StUG, worin es konkret heißt:

„§ 32 – Verwendung von Unterlagen für die politische und historische Aufarbeitung:

(1) Für die Forschung zum Zwecke der politischen und historischen Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes oder der Herrschaftsmechanismen der ehemaligen Deutschen Demokratischen Republik oder der ehemaligen sowjetischen Besatzungszone sowie für Zwecke der politischen Bildung stellt der Bundesbeauftragte auf Antrag folgende Unterlagen zur Verfügung:
[…]
3. Unterlagen mit personenbezogenen Informationen über
– Mitarbeiter des Staatssicherheitsdienstes, soweit es sich nicht um Tätigkeiten für den Staatssicherheitsdienst vor Vollendung des 18. Lebensjahres gehandelt hat, oder
– Begünstigte des Staatssicherheitsdienstes. […]"

Weiter in § 32 Abs. 3 Satz 2 StUG: Personenbezogene Informationen dürfen nur veröffentlicht werden, wenn es sich um Informationen handelt über – Mitarbeiter des Staatssicherheitsdienstes, soweit diese nicht Tätigkeiten für den Staatssicherheitsdienst vor Vollendung des 18. Lebensjahres betreffen, oder – Begünstigte des Staatssicherheitsdienstes.
Aus datenschutzrechtlicher Sicht ist darauf hinzuweisen, dass das Bundesdatenschutzgesetz (BDSG) dann keine Anwendung findet, wenn einschlägige spezielle Rechtsnormen existieren. Im vorliegenden Fall ist in § 43 StUG ausdrücklich geregelt, dass die Regelungen dieses Gesetzes den Vorschriften über die Zulässigkeit der Übermittlung personenbezogener Informationen in anderen Gesetzen vorgeht. Das Bundesdatenschutzgesetz finde mit Ausnahme der Vorschriften über die Datenschutzkontrolle keine Anwendung, soweit nicht in § 6 Abs. 9 und § 41 Abs. 1 Satz 2 dieses Gesetzes etwas anderes bestimmt ist.
Das hat der TLfDI dem Sohn in dieser Form schriftlich übermittelt.

Im Ergebnis beurteilt sich die Zulässigkeit der Veröffentlichung von Namen, Vornamen und Geburtsdaten von ehemaligen Mitarbeitern des MfS nicht nach den Bestimmungen des BDSG, sondern nach den spezielleren Regelungen des StUG.

2.22 Auskunftsverlangen – datenbewusster Bürger unterstützt TLfDI!

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Bürgers über eine nicht erteilte Auskunft über seine bei dem Unternehmen gespeicherten personenbezogenen Daten. Darüber hinaus wollte der Bürger von dem Unternehmen wissen, an wen seine personenbezogenen Daten weitergeben wurden.
Hintergrund des Auskunftsersuchens gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) war der Erhalt einer unerwünschten Phishing-Mail. Weil es sich um einen im Umgang mit seinen personenbezogenen Daten sehr umsichtigen Bürger handelte, konnte die mögliche Ursache für den Ursprung dieser Mail abgeleitet werden. Denn dieser legte für jeden Händler, bei dem er bestellte, einen Account mit einer neuen, extra für diesen Zweck erstellten E-Mailadresse an. Die E-Mailadresse setzte sich dann aus dem Namen des Internetshops und einer zufälligen, mindestens sechsstelligen Zahl zusammen. Somit konnte der Bürger anhand der an ihn adressierten E-Mailadresse nachvollziehen, welcher Online-Shop möglicherweise seine E-Mail weitergegeben hatte.
Der TLfDI wandte sich daher an das Unternehmen, wies auf den Sachverhalt hin und klärte das Unternehmen über die Auskunftspflichten nach § 34 BDSG auf. Danach ist die verantwortliche Stelle, also das Unternehmen, welches die personenbezogenen Daten gespeichert hat, verpflichtet, dem Betroffenen auf Verlangen darüber Auskunft zu erteilen, welche Daten diese über den Betroffenen gespeichert hat, woher diese kamen und an wen diese weitergegeben wurden. Ebenfalls hat das Unternehmen über den Zweck der Speicherung Auskunft zu erteilen. Bei nicht, nicht richtiger oder nicht vollständiger Erteilung dieser Auskunft kann die verantwortliche Stelle sogar mit einer Geldbuße von bis zu 50.000 Euro rechnen, vergleiche § 43 Abs. 1 Nr. 8a BDSG.
Das Unternehmen wurde aufgefordert, dieser Pflicht nachzukommen. Daneben wurde das Unternehmen auf § 42a BDSG hingewiesen. Dieser verpflichtet verantwortliche Stellen, bei Abhandenkommen bestimmter Daten, die Betroffenen und die Aufsichtsbehörde zu informieren (siehe auch Nummer 2.19).
Durch das Anschreiben des TLfDI klärte sich der Fall komplett auf. Das Auskunftsersuchen war wegen längerer Krankheit des Einzelun-

ternehmers noch nicht beantwortet. Dies ist zwischenzeitlich geschehen. Ebenfalls nahm das Unternehmen das Anschreiben des TLfDI zum Anlass, die IT-Systeme auf einen Fremdzugriff hin überprüfen zu lassen. Diese Überprüfung, deren Protokoll dem TLfDI vorliegt, kam zum Ergebnis, dass keine Daten abgeflossen waren.

Den Betroffenen steht gemäß § 34 BDSG ein Auskunftsrecht gegenüber der verantwortlichen Stelle zu. Wird ein Auskunftsbegehren ignoriert, kann der Betroffene bei dem TLfDI als zuständige Aufsichtsbehörde für den Datenschutz eine Beschwerde einreichen. Dem Auskunftsverpflichteten droht ein Bußgeldverfahren.

2.23 Kindsvater versus Anwaltsgeheimnis

Ein Vater beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Rechtsanwältin der Mutter seines Kindes, weil diese nach seiner Meinung im Rahmen einer gerichtlichen Sorgerechtsstreitigkeit über ihn Falsches erzählt habe. Im Übrigen vertrat er die Auffassung, die Rechtsanwältin unterliege der Schweigepflicht auch in Bezug auf seine Person. Von dieser habe er sie nicht entbunden und er habe auch keine Einwilligung erteilt, dass sie in der Sorgerechtsstreitigkeit vor Gericht Angaben über ihn machen dürfe. Bei allem Verständnis für die emotionale Lage des Beschwerdeführers konnte der TLfDI dem Anliegen nicht nachkommen.
Die Rechtsanwältin unterliegt selbstverständlich der Verschwiegenheit über die in Wahrnehmung ihres Mandats zu verarbeitenden personenbezogenen Daten. Da der Beschwerdeführer selbst aber nicht zur Mandantschaft der Rechtsanwältin zählte, durften seine Daten – soweit im Zusammenhang mit der Vertretung im gerichtlichen Verfahren erforderlich – verarbeitet werden. Die personenbezogenen Daten als Vater sind als Daten Dritter zwangsläufig zu dem Mandat der Antragsgegnerin (der Kindsmutter) gespeichert, wenn es sich um eine Auseinandersetzung bezüglich des Sorgerechts für das gemeinsame Kind handelt. Den Kindsvater in einem solchen Zusammenhang überhaupt nicht berücksichtigen zu dürfen, wie der Beschwerdeführer meinte, wäre äußerst weltfremd.
In Vertretung eines Mandanten ist es gerade die Aufgabe eines Rechtsanwalts, das für die zu vertretenden Mandanten Günstige und Entscheidungserhebliche vorzutragen. Eine Überprüfung auf den

Wahrheitsgehalt ist dem TLfDI weder aus rechtlichen noch aus sachlichen Gründen möglich. Da die Daten im gerichtlichen Verfahren verlautbart wurden, ist es Sache des Gerichts, zu entscheiden, ob dem Vorbringen Glauben zu schenken ist und es gegebenenfalls als beweiserheblich genutzt werden kann. Eine Überprüfung durch den TLfDI ist bei Gerichten nicht möglich, wenn es um rechtsprechende Tätigkeit (wie hier) geht. Dieser Bereich ist von der Kontrolle durch den TLfDI ausgenommen, § 2 Abs. 6 Thüringer Datenschutzgesetz.
Damit gab sich der Beschwerdeführer allerdings nicht zufrieden. Er verlangte weiteres Vorgehen des TLfDI gegen die Rechtsanwältin.
Diesem Begehren konnte der TLfDI aus folgenden Gründen nicht zum Durchbruch verhelfen:
Die Aufsicht nach § 38 Bundesdatenschutzgesetz (BDSG) besteht unabhängig von etwaigen Berufs- und Amtsgeheimnissen (vergleiche § 38 Abs. 4 Satz 3, § 24 Abs. 6, Abs. 2 BDSG). Grundsätzlich unterliegen damit auch Geheimnisträger im Sinne des § 203 Strafgesetzbuchs (StGB) ebenso uneingeschränkt der Datenschutzaufsicht nach § 38 BDSG wie jede andere nicht-öffentliche Stelle. Die Aufsichtsbehörde hat folglich auch freiberuflich Tätige zu kontrollieren. Soweit neben den allgemeinen Regeln des BDSG für diese Personengruppen bereichsspezifische Schweige- und Geheimhaltungspflichten gelten, werden hierdurch die allgemeinen Regeln des BDSG allenfalls punktuell berührt. Aufgrund der bisherigen Rechtsprechung ist die Kontrolltätigkeit der Datenschutzaufsichtsbehörden bei Rechtsanwälten eingeschränkt. Rechtsanwälte können Auskünfte gegenüber der datenschutzrechtlichen Aufsichtsbehörde verweigern, wenn dadurch das Mandantengeheimnis verletzt werden könnte. Dies wird mit dem besonderen Status der Rechtsanwälte als Organe der Rechtspflege begründet. Insoweit zeigt sich hier ein Unterschied zu den anderen Berufsgeheimnisträgern.
Der TLfDI wies den Beschwerdeführer auf die Rechtslage und darauf hin, dass es ihm selbstverständlich frei stand, die für die Berufsethik zuständige Rechtsanwaltskammer mit der Angelegenheit zu befassen. Ein Rechtsmittel gegen die Entscheidung des TLfDI steht nicht zur Verfügung, der Beschwerdeführer musste sich also mit der Antwort des TLfDI abfinden.

Der TLfDI ist auch Datenschutzaufsichtsbehörde für Rechtsanwälte und geht selbstverständlich Beschwerden von Betroffenen nach. Im Rahmen einer datenschutzrechtlichen Prüfung bei Rechtsanwälten

kann von diesen nicht verlangt werden, ihre Schweigepflicht gegenüber ihrer Mandantschaft zu verletzen und sich damit strafbar zu machen. Auch wenn die gegnerische Seite meint, ein Rechtsanwalt habe unrichtige personenbezogene Daten über sie verarbeitet, kann dies vom TLfDI insoweit weder aus rechtlichen noch tatsächlichen Gründen überprüft werden.

2.24 Die Transparenz des Erneuerbare-Energien-Gesetzes (EEG)

Ein Anlagenbetreiber einer Photovoltaikanlage hat sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt und um Überprüfung der Veröffentlichungsvorschriften der Netzbetreiber gebeten. Konkret ging es dem Anlagenbetreiber darum zu erfahren, auf welcher gesetzlichen Grundlage die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten der Anlagenbetreiber (Anlagenstammdaten) erfolgte und was diese für jedermann zugängliche Veröffentlichung dieser Daten im Internet rechtfertigen könnte. Hintergrund war die jedermann im Internet zugängliche Excel-Tabelle eines Netzbetreibers. In dieser Tabelle waren unter anderem der Energieträger, der Standort der Anlage (Ort/Gemarkung, PLZ, Straße/Flurstück, Nummer), die Einspeisemenge und die ausgezahlte Vergütung (inkl. Marktprämie) aufgeführt. Vor allem beschwerte sich der Anlagenbetreiber wegen der Veröffentlichung der Straße und Hausnummer sowie der PLZ und des Orts. Denn nun konnte jeder Nachbar ihm genau vorrechnen, was er im Jahr als Erlös erhalten hatte.
Daraufhin forderte der TLfDI den Netzbetreiber um Mitteilung der Rechtsgrundlage für die Veröffentlichung der Anlagestammdaten der Anlagenbetreiber auf. Denn nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Der Netzbetreiber teilte dem TLfDI mit, dass er nach § 77 Abs. 1 Erneuerbare-Energien-Gesetz (EEG), gültig seit dem 1. August 2014, dazu verpflichtet gewesen sei. Danach sind Netzbetreiber verpflichtet, die für die Ermittlung der auszugleichenden Energiemengen und Vergütungszahlungen erforderlichen Angaben im Internet zu veröffentlichen.
Dafür haben die Anlagenbetreiber nach § 71 EEG dem zuständigen Netzbetreiber insbesondere den Standort und die installierte Leistung

sowie alle Daten zur Erstellung der Abrechnung des Vorjahres zur Verfügung zu stellen. Innerhalb der Literatur und auch bei der Bundesnetzagentur bestand Einigkeit darüber, dass zum Standort eine konkrete Anschrift (Ort, PLZ, Straße, Hausnummer) gehört. Etwas anderes gilt nur dann, wenn der Anlage keine Anschrift zugeordnet werden kann, so z. B. bei Freiflächenanlagen, hier ist dann die Bezeichnung der Gemarkung und des Flurstücks ausreichend gewesen. Ziel dieser Veröffentlichungsvorschriften war die Schaffung von Transparenz in Hinblick auf die Ermittlung der EEG-Umlage, welche durch die Öffentlichkeit getragen wird. Denn soweit die Öffentlichkeit durch diese Umlage belastet wird, sollte diese auch in die Lage versetzt werden, nachzuvollziehen, wofür und inwieweit diese Gelder verwendet werden.
Im Ergebnis stellte der TLfDI fest, dass der Netzbetreiber mit der Veröffentlichung einer gesetzlichen Verpflichtung nachkam und dies im Sinne des § 4 Abs. 1 BDSG durch eine andere Rechtsvorschrift gerechtfertigt war. Im Falle der Nichterfüllung der Veröffentlichung von den Netzbetreiber kann das sogar eine Aufsichtsmaßnahme der Bundesnetzagentur gemäß §§ 65 ff. Energiewirtschaftsgesetz (EnWG) nach sich ziehen.
Dieses Ergebnis teilte der TLfDI dem Anlagenbetreiber mit.

Aus Gründen der Transparenz und der Überprüfbarkeit verpflichtet das Erneuerbare-Energien-Gesetz (EEG) die Stromnetzbetreiber dazu, die Daten zu Standort, Stromertrag und Stromvergütung der ihnen gemeldeten Anlagen unverzüglich auf ihren Internetseiten in einer Form zu veröffentlichen, „dass eine sachkundige Person diese ohne weitere Hilfe auswerten kann“. Dies stellt im Sinne des § 4 Abs. 1 BDSG eine spezialgesetzliche Erlaubnisnorm dar.

2.25 Zulässige Weitergabe von Kundendaten bei Abmahnung von Dritten wegen illegalem Filesharing

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für Datenschutz und die Informationsfreiheit (TLfDI) die Frage eines Vereins, unter welchen Voraussetzungen Namen und möglicherweise Adressen von Personen an die Vermieter von Unterkünften weitergegeben werden dürften, denen der Verein im Rahmen einer Veranstaltung Unterkünfte bei diesen vermittelt hatte. Der Verein gab gegenüber dem TLfDI an, dass eine Weitergabe der Daten nur in

den Fällen erfolgen sollte, bei denen die Personen den Internetzugang der Unterkunft zu illegalen Zwecken genutzt hätten und die Vermieter dadurch, als Anschlussinhaber, Abmahnungen Dritter wegen illegalen Filesharings erhalten hätten. Da es sich bei der Anfrage des Vereins nur um eine allgemeine Anfrage handelte, konnte der TLfDI hier Abwägungsfragen nicht für den Einzelfall prüfen.
Ursprünglich wurden die Namen und Adressdaten zur Organisation der Veranstaltung erhoben. Grundsätzlich gilt im Datenschutzrecht das Prinzip der Zweckbindung. Werden Daten also für einen Zweck erhoben, können sie nicht einfach so für einen anderen Zweck verarbeitet werden. Allerdings gibt es hierzu gesetzlich normierte Ausnahmen.
Nach § 28 Abs. 2 Nr. 2a Bundesdatenschutzgesetz (BDSG) ist die Übermittlung oder Nutzung für einen anderen Zweck zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. In der dem TLfDI vorgetragenen Konstellation sprach, vorbehaltlich von Abwägungsfragen im konkreten Einzelfall, vieles für das Vorliegen dieser Voraussetzungen. Wenn feststeht, dass der vermittelte Mieter Rechtsverstöße bei der Nutzung des Internetanschlusses des Vermieters begangen hat, kann der Verein dessen personenbezogene Daten, soweit diese für die Verteidigung gegen die Abmahnung erforderlich sind, an den Vermieter herausgeben. Übermittlungsnorm wäre in einem solchen Fall § 28 Abs. 2 Nr. 2a BDSG, da die Daten zu anderen Zwecken, als bei der Erhebung festgelegt wurde, an den jeweils betroffenen Anschlussinhaber (Vermieter) übermittelt werden würden. In einer Übermittlung nur zur Abwehr von Abmahnungen wäre ein berechtigtes Interesse von Dritten, vorliegend der Anschlussinhaber, an der Übermittlung i. S. d. § 28 Abs. 2 Nr. 2a BDSG zu sehen. Darüber hinaus hätte bei einer rechtswidrigen Nutzung des Internetzugangs kein Grund zur Annahme bestanden, dass die Betroffenen, vorliegend die Mieter, ein schutzwürdiges Interesse am Ausschluss der Übermittlung gehabt hätten.
Da dem TLfDI keine weiteren Informationen von dem Verein zur Verfügung gestellt wurden, konnte die Anfrage nur in diesem abstrakten Rahmen beantwortet werden.

Nach § 28 Abs. 2 Nr. 2a Bundesdatenschutzgesetz (BDSG) ist die Übermittlung oder Nutzung für einen anderen Zweck zulässig (zweckfremd), soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

2.26 Personalausweiskopie auch nicht bei Pflicht zur Datenerhebung!

Ein Kunde beschwerte sich darüber, beim Kauf eines Desinfektionsmittels für seinen Pool eine Personalausweiskopie hinterlegen zu müssen. Auf Nachfrage teilte der Verkäufer ihm mit, dass der gekaufte Artikel Bestandteile enthalte, die zum Bomben bauen geeignet wären und er verpflichtet sei, die Angaben zum Käufer durch Vorlage des Personalausweises zu prüfen. Zudem wurde die Kopie des Ausweises an die Rechnung des Kunden geheftet. Bei diesem Produkt handelte es sich um eine Flüssigkeit, welche auf Aktivsauerstoffbasis mit einer Konzentration von mehr als 12 % Wasserstoffperoxid versehen war.
Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsnorm dies erlaubt oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Die Feststellung der Identität wird nach § 3 Abs. 1 Satz 4 der Chemikalien-Verbotsverordnung (ChemVerbotsV) in diesem Fall angeordnet. Danach hat der Verkäufer ein Abgabebuch zu führen, welches den Namen und die Anschrift des Erwerbers beinhalten muss. Allerdings war das Kopieren des Personalausweises dennoch unzulässig. Das Abgabebuch war vom Verkäufer mindestens fünf Jahre nach der letzten Eintragung aufzubewahren. Nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) darf die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich nach Maßgabe der §§ 18 bis 20 PAuswG erfolgen (siehe auch Nummer 2.7). Nach § 20 Abs. 2 PAuswG darf dieser jenseits des elektronischen Identitätsnachweises nicht zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Hierunter zählt auch das Kopierverfahren.

Der Verkäufer stellte auf Forderung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfertigung der Personalausweiskopien ein. Vielmehr wurden jetzt nur noch der Name und die Anschrift des Endkunden nach Vorlage des Personalausweises erhoben. Das zu führende Abgabebuch über das streitgegenständliche Produkt wurde in einem Stahlschrank des zusätzlich mit Alarmanlage und Sicherheitsdienst bewachten Gebäudes eingeschlossen, sodass sich niemand Zugang zu diesen sensiblen Daten verschaffen konnte.

Auch wenn eine gesetzliche Grundlage gegeben ist, personenbezogene Daten der Kunden zu erheben und zu verarbeiten, muss sich der Unternehmer auf das notwendigste Maß beschränken. Zu Identifikationszwecken dürfen nach § 20 Abs. 2 PAuswG nur die hierfür erforderlichen Daten erhoben und mit dem Personalausweis abgeglichen werden.

2.27 Personalausweiskopie? Schrott! – Fortsetzung

Bereits mit der Übernahme des nicht-öffentlichen Bereichs vom Thüringer Landesverwaltungsamt im Dezember 2011 hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einen hartnäckigen Fall der Anfertigung von Personalausweiskopien bei einem Metall-Recycling-Unternehmen zu bearbeiten. Wie schon im 1. Tätigkeitsbericht des TLfDI zum Datenschutz: nicht-öffentlicher Bereich dargestellt, hielt das Unternehmen das Ablichten des Personalausweises für erforderlich, um den Nachweis- und Dokumentationspflichten der Finanzbehörden ordnungsgemäß nachzukommen (s. a. 1. TB TLfDI: Nicht-öffentlicher Bereich [3.48]). Nach § 160 der Abgabenordnung (AO) ist der Zahlungsempfänger bei einem Schrott-Ankauf zweifelsfrei zu benennen. Andernfalls werden die Betriebsausgaben des Unternehmens steuerlich nicht berücksichtigt. Allerdings werde auf Nachfrage bei der zuständigen Finanzbehörde die Kopie des Bundespersonalausweises nicht verlangt. Die von dem Metall-Recycling-Unternehmen betriebene Datenerhebung war damit nicht erforderlich. Eine Rechtsgrundlage für diese Datenerhebung bestand demnach weder nach § 160 AO noch nach § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zur Wahrung berechtigter Interessen der verantwortlichen Stelle.

Nach mehrfacher Aufforderung des TLfDI, keine Personalausweiskopien mehr anzufertigen und der Androhung zum Erlass einer Anordnung gemäß § 38 Abs. 5 BDSG, welche auf die Herstellung datenschutzkonformer Zustände abzielt, wurde die Anfertigung von Personalausweiskopien tatsächlich eingestellt. Dem Metall-Recycling-Unternehmen wurde vorgeschlagen, zur Erfassung der für die Identifikation erforderlichen Daten ein Formblatt zu verwenden. Das Metall-Recycling-Unternehmen folgte dem Vorschlag, die Erfassung der erforderlichen Daten über ein Formblatt vorzunehmen und legte dies dem TLfDI nach mehrfacher Aufforderung vor. Allerdings hielt das Metall-Recycling-Unternehmen auch die Erhebung von personenbezogenen Daten für erforderlich, die durch das Gesetz nicht gefordert wurden. So wurden folgende Daten abgefragt: „Name“, „Vorname“, „Straße“, „PLZ/Ort“, „Geburtsdatum“, „Geburtsort“, „Staatsangehörigkeit“, „Personalausweisnummer“ und „Gültig bis“. Weiterhin war der Zusatz „Die von mir gemachten Angaben sind freiwillig erfolgt.“ auf dem Formblatt aufgedruckt.
Das Metall-Recycling-Unternehmen hatte die o. g. Daten aufgrund der gesetzlichen Anordnung des § 143 Abs. 3 Nr. 2 AO erhoben und gespeichert. Hiernach war es notwendig, den Wareneingang gesondert aufzuzeichnen. Dabei mussten diese Aufzeichnungen nach § 143 Abs. 3 Nr. 2 AO den Namen oder die Firma und die Anschrift des Verkäufers enthalten. Eine Anordnung, die sonstigen von dem Metall-Recycling-Unternehmen erhobenen Daten zu erheben, enthielt § 143 AO nicht. Darüber hinaus ist es Sinn und Zweck des § 160 AO, den tatsächlichen Empfänger von Geldleistungen dem Finanzamt gegenüber identifizierbar zu machen. Dieser Zweck wurde jedoch durch die zusätzliche Erhebung der Angaben „Geburtsdatum“, „Geburtsort“, „Staatsangehörigkeit“, „Personalausweisnummer“ und „Gültig bis“ nicht erreicht. Zwar wies das Unternehmen auf die „Freiwilligkeit“ der Angaben hin, der Hinweis allein begründete eine solche aber nicht. Damit war es dem Metall-Recycling-Unternehmen weder erlaubt noch angeordnet, die o. g. Datenkategorien bei den Verkäufern zu erheben und zu speichern.
Trotz längerem Austausch über die Rechtsauffassung des TLfDI folgte das Metall-Recycling-Unternehmen dieser nicht. Der TLfDI war daher gezwungen, eine Anordnung gemäß § 38 Abs. 5 Satz 1 BDSG zu erlassen. Diese zielte darauf ab, dass die Angaben „Geburtsdatum“, „Geburtsort“, „Staatsangehörigkeit“, „Personalausweisnummer“ und „Gültig bis“ nicht länger erhoben wurden und der

Hinweis „Die von mir gemachten Angaben sind freiwillig erfolgt." entfernt wurde. Das Unternehmen hat Rechtsmittel eingelegt. Der TLfDI wird über den Ausgang des Verfahrens berichten.

Ein Anordnungsbescheid nach § 38 Abs. 5 Satz 1 BDSG stellt einen Verwaltungsakt nach § 35 des Verwaltungsverfahrensgesetzes dar. Vor Erlass eines Anordnungsbescheides ist die verantwortliche Stelle in der Sache anzuhören. Es muss eine angemessene Frist zur Mängelbeseitigung gesetzt werden, bevor die Untersagung einzelner Verfahren getroffen werden kann, § 38 Abs. 5 Satz 2 BDSG.

2.28 Keine vollständige Mieterselbstauskunft bei Besichtigungsterminen

Wer kennt das nicht – bevor man eine Wohnung anmieten kann, muss das Leben offengelegt werden. Jeder, der auf Wohnungssuche ist, muss umfangreiche Fragebögen zu Person, Hobbies, Familien- und Berufsleben und zur finanziellen Situation ausfüllen; am besten auch gleich noch ein polizeiliches Führungszeugnis dazu vorlegen. Das Ganze natürlich, bevor überhaupt eine Wohnung besichtigt werden kann. Das geht eindeutig zu weit!
Im April 2014 wurde eine Thüringer Immobilienverwaltung auf derartige Fragebögen kontrolliert. Wie soll es auch anders sein, der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) fand Zustände vor, wie sie jeder kennt, der bereits eine Wohnung gesucht hat. Sämtliche Daten, ähnlich wie eingangs dargestellt, wurden vor Vermietung und Besichtigung einer Wohnung erhoben. Eine derartige Datenerhebung bedarf nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) einer wirksamen Einwilligung des betroffenen Personenkreises, sprich der potenziellen Mieter, oder einer gesetzlichen Grundlage. Die Verwendung von Einwilligungserklärungen für Mietinteressenten in Formularen zur Selbstauskunft ist nach Ansicht des TLfDI grundsätzlich nicht als das richtige Mittel zur Datenerhebung anzusehen. Eine wirksame Einwilligung erfordert nach § 4a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Dem Mietinteressenten wird bei Mieterselbstauskünften häufig suggeriert, er habe bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht. Tatsächlich ist dem in der Realität nicht so. Zumindest der Eindruck ist vorhanden, dass der, der die geforderten Daten nicht liefert, bei der Aus-

wahlentscheidung des Vermieters keine Chance hat. Deswegen entfällt oftmals diese vermeintliche Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommen kann. Unabhängig davon, dass das formularmäßige Abfragen nach den vorstehenden Ausführungen nicht als vorrangiges Mittel angesehen werden kann, ist es geboten, Fragen auf das erforderliche und datenschutzrechtlich zulässige Maß zu beschränken.
Da aus den dargelegten Gründen die erteilte Einwilligung in der Regel nicht wirksam ist, richtet sich die Zulässigkeit der Erhebung einer Selbstauskunft im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht dann ein vorvertragliches Schuldverhältnis zum künftigen Vermieter, sodass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Hiernach ist das Erheben personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Im Rahmen dieser dann vorzunehmenden Erforderlichkeitsprüfung kommt es darauf an, ob von Seiten des Interessenten Offenbarungspflichten bestehen bzw. ob von Vermieterseite aus zulässige Fragen gestellt werden. Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen des Mietanwärters am Ausschluss der Datenerhebung bestehen. Dabei geht es nicht nur um eine datenschutzrechtliche, sondern auch um eine grundrechtliche Problematik der richtigen Abwägung zwischen Mieter- und Vermieterinteressen und damit um die Frage nach der Zulässigkeit oder Unzulässigkeit bestimmter Fragen.
In der verwendeten Mieterauskunft wurden Daten vom Mietinteressenten erfragt, die zu Beginn der Mietvertragsverhandlungen (noch) nicht erforderlich sind und die teilweise auch in den weiteren Stadien der Vertragsanbahnung unzulässig sind, da sie das Mietverhältnis nicht betreffen. Zunächst muss bezüglich der Datenerhebung zwischen drei Zeitpunkten differenziert werden (siehe auch Anlage 10)

(a) dem Besichtigungstermin,

(b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und
(c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Deshalb ist ein dreistufiges Verfahren zur formularmäßigen Abfrage von Mieterdaten empfehlenswert. Das kontrollgegenständliche Formular hat nicht nach den einzelnen Stufen unterschieden. Eine solche Unterscheidung (ggf. auch in gesonderten Formularen) ist hier jedoch bei der Art der Fragestellung notwendig, um die Mieterselbstauskunft datenschutzrechtlich zulässig anwenden zu dürfen.
Bei einer formularmäßigen Mieterselbstauskunft muss dem potentiellen Mieter ersichtlich sein, dass er zum **Besichtigungstermin** nur die folgenden Daten angeben muss:

- Daten zur Identifikation des Mietinteressenten, hierzu zählen dessen Vorname und Nachname sowie die Adresse (ggf. Telefonnummer zu weiteren Terminabsprachen) und
- Angaben zur Haltung von größeren Tieren (unzulässig ist die pauschale Frage nach Haustieren jeglicher Art, also auch Kleintieren).

Dies war zum Kontrollzeitpunkt im Formular der kontrollierten Immobilienverwaltung nicht gewährleistet. Bei der augenblicklichen Handhabung der Mieterselbstauskunft erweckte diese beim Interessenten den Eindruck, dass er der Immobilienverwaltung zum Besichtigungstermin den vollständig ausgefüllten Vordruck zu übergeben hat. Eine datenschutzrechtlich zulässige Auslegung einer Selbstauskunft setzt hingegen voraus, dass dem Bewerber bewusst gemacht wird, dass andere Fragen des Vordruckes erst zum Tragen kommen, wenn der Mietinteressent dem Vermieter zu verstehen gibt, ein konkretes Interesse zur Anmietung dieses Objektes zu besitzen.

Die zweite Stufe, die **vorvertragliche Phase**, tritt ein, wenn der Mietinteressent dem künftigen Vermieter mitteilt, das Mietobjekt anmieten zu wollen. Dann sind folgende Fragen zulässig:

- Anschrift und Telefonnummer des Mietinteressenten,

- Angaben zu den im Haushalt lebenden Personen (erforderlich für die Beurteilung der Wohnungsnutzung),
- eröffnetes Insolvenzverfahren, Abgabe einer eidesstattlichen Versicherung, Räumungstitel wegen Mietzinsrückständen,
- Einkommensverhältnisse,
- Angaben zum Arbeitgeber, zum Beschäftigungsverhältnis und zum Beruf.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden und sind damit zulässig, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben zu diesen Personen dürfen nicht eingeholt werden. Aus diesem Grunde sind die Fragen nach deren Namen, den Verwandtschaftsgraden, den Geburtsdaten, den Einkommensverhältnissen und den Berufen der Mitbewohner unzulässig und zu streichen gewesen. Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist dagegen zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen. Die Frage nach Räumungstiteln wegen Mietzinsrückständen ist nur dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben kann, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnisses mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht. Erkundigungen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchgeführt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, sind daher zulässig. In dem kontrollgegenständlichem Formular wurde nicht auf die zeitliche Nähe zum Räumungsverfahren abgestellt. Ohne eine zeitliche Fristbegrenzung auf höchstens fünf Jahre ist diese und die Frage nach allgemeinen Mietrückständen jedoch unzulässig. Das Erfragen der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens ist auch die Angabe einer bestimmten Betragsgrenze durch den Mietinteressenten ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird.

Verdienst-Anfragen beim Arbeitgeber sind daher nicht erforderlich und beim Betroffenen selbst einzuholen. In der geprüften Selbstauskunft wurde dem potentiellen Mieter nicht ermöglicht, durch Festlegung eines Mindestbetrages, der ihm für die Mietzahlungsverpflichtung zur Verfügung steht, seiner Auskunftspflicht zu genügen. Insoweit war das Formular ebenfalls als unzulässig zu bewerten. Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Dies gilt nur für den derzeit ausgeübten, nicht aber für den erlernten Beruf. Welchen Beruf der Interessent erlernt hat, ist für seine Eignung als Mieter nicht entscheidend. Auch die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu befriedigen. Fragen nach der Art oder der Dauer der Beschäftigung können nur relevant und damit unter Umständen zulässig sein, wenn es sich dabei um eine Ausbildung, eine Probezeit oder ein befristetes Beschäftigungsverhältnis handelt. Auch dahingehend war das geprüfte Formular nicht einwandfrei und bedurfte einer Änderung.
Die Abfrage der folgenden Angaben ist auf jeden Fall in allen Stufen **unzulässig** und für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich:

- Bankverbindung,
- Familienstand,
- Vorstrafen/strafrechtliche Ermittlungsverfahren,
- Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit,
- Angaben zu bisherigen Vermietern,
- Musikinstrumente,
- Raucher/Nichtraucher,
- Fragen nach einer Privathaftpflichtversicherung und nach Grundeigentum.

In der dritten Phase, der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten, möchte der künftige Vermieter nun mit einem Mietinteressenten für eine konkrete Wohnung einen Mietvertrag abschließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten

(Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein:

- Nachweise zu den Einkommensverhältnissen,
- Auskünfte von Auskunfteien – Sonderfall!, Auskünfte bei einer Auskunftei,
- Nachweis des Arbeitsplatzes,
- Mietbürgschaft.

Der künftige Vermieter kann bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen in der vorvertraglichen Phase darauf hinweisen, dass für den Fall einer positiven Entscheidung für den Mietinteressenten – quasi unmittelbar vor Unterzeichnung des Vertrags – noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z. B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben. Als Nachweis ist auch eine Bescheinigung des Arbeitgebers ausreichend, dass die Angaben des Mietinteressenten bezüglich der Angabe einer bestimmten Nettobetragsgrenze, die überschritten wird, zutreffend sind. Wegen des Informationsbedürfnisses des Vermieters ist er unter bestimmten Voraussetzungen berechtigt, auch selbst Auskünfte bei Auskunfteien einzuholen. Das Abfragen von Bonitätsinformationen über Mietbewerber bei Auskunfteien wie zum Beispiel der SCHUFA oder Creditreform durch den Vermieter sind nur unter den gesetzlichen Voraussetzungen des § 29 Abs. 2 Nr. 1a BDSG und auch nur in eingeschränktem Umfang zulässig. Selbstauskünfte, die Mietinteressenten bei Auskunfteien selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse, als für eine Beurteilung durch den Vermieter erforderlich sind. Schon aus diesem Grund wäre die Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig. Zulässig sind in diesem Fall jedoch ausschließlich Auskünfte über solche Daten, die Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen enthalten sowie sonstige Daten zu negativem Zahlungsverhalten, bei denen die dem Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und eine Bagatellgrenze von 1.500 Euro überschritten wird (s. Beschluss der Auf-

sichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“ v. 22. Oktober 2009 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/27012014_OHSelbstauskuenfteMietinteressenten.pdf?__blob=publicationFile&v=1).

In unserem geprüften Formular waren keine Einschränkungen vorgenommen und anlassunabhängig Auskünfte der Mieter zu gewähren und somit abzuändern. Bei der Vermietung der Wohnung an Studenten und Auszubildende macht der Vermieter den Abschluss des Mietvertrags häufig davon abhängig, dass die Bürgen für die Verpflichtungen aus dem Mietvertrag aufkommen. Bürgen können Institutionen (wie zum Beispiel Banken) oder auch Personen (zum Beispiel Verwandte oder Arbeitgeber) sein. Erforderlich für die Begründung eines Mietvertragsverhältnisses sind die Daten des Bürgen, die Aufschluss über seine Identität sowie seine finanzielle Leistungsfähigkeit und damit letztlich seine Tauglichkeit als Sicherungsmittel geben, soweit der Bürge eine natürliche Person ist. Hierzu gehören der vollständige Name des Bürgen sowie Angaben zu seinem Beruf und seinem Nettoeinkommen. Die Bürgschaft ist nur wirksam, wenn sie nach § 766 Bürgerliches Gesetzbuch (BGB) schriftlich erklärt und das Schriftstück dem Vermieter übergeben wurde. Nicht erforderlich ist die Vorlage einer Bürgschaftsurkunde vor Abschluss des Mietvertrages. Der potentielle Mieter ist deswegen erst mit Beginn des Mietverhältnisses verpflichtet, eine solche Bürgschaftsurkunde vorzulegen. Wird sie nicht vorgelegt, hat der Vermieter ein Zurückbehaltungsrecht nach §§ 273, 274 BGB. Nach § 273 BGB hat der Vermieter das Recht, die Übergabe des zu vermietenden Wohnraums bis zur Vorlage der Bürgschaftsurkunde zu verweigern. Außerdem kann der Vermieter das Mietverhältnis nach Prüfung des Einzelfalls nach § 573 Abs. 2 Nr. 1 BGB kündigen, wenn ihm die Bürgschaftsurkunde nicht übergeben wird.

Die Immobilienverwaltung wurde aufgefordert, das Formular zur Mieterselbstauskunft zu überarbeiten, unzulässige Fragen zu streichen, die bis dahin unzulässig gespeicherten Daten unwiederbringlich zu löschen und ein angepasstes Formblatt vor Veröffentlichung

im Internet dem TLfDI vorzulegen. Nachdem der TLfDI die datenschutzrechtlich unzulässigen Fragen dargestellt hatte, hatte das betroffene Unternehmen, die streitbefangene Mieterselbstauskunft entsprechend angepasst.

Dem TLfDI ist bewusst, dass sich ein Wohnungssuchender nicht mit dem vermakelnden Unternehmen oder dem Vermieter selbst in Streit begeben wird, welche Daten erhoben werden dürfen oder nicht. Der Wohnungssuchende kann sich bei Missständen jedoch jederzeit an den TLfDI wenden. Dieser kann, jedenfalls so lange, wie es nicht zu einem gerichtlichen Verfahren kommt, die Anonymität des sich Beschwerenden wahren.

2.29 Was darf man in der Mieterselbstauskunft fragen?

Im Rahmen einer Kontrolle stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) fest, dass auf der Homepage einer Haus- und Immobilienverwaltung als „Download“ eine Mieterselbstauskunft, eine Mietschuldenfreiheitsbescheinigung (Bestätigung des Vermieters über termingerechte Mietzahlung des Mieters) sowie eine Einwilligungserklärung zur Bonitätsprüfung den Mietinteressenten zur Verfügung standen, die aber nicht den datenschutzrechtlichen Bestimmungen entsprachen.
Zunächst teilte der TLfDI der Haus- und Immobilienverwaltung mit, dass das Bundesdatenschutzgesetz (BDSG) den Einzelnen davor schützt, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, vergleiche § 1 Abs. 1 BDSG. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Diese Regelung gilt auch bei der Vermietung von Wohnraum und den in diesem Zusammenhang zu erhebenden Daten. Für die von der Haus- und Immobilienverwaltung mittels der vorgefundenen Formulare durchgeführte Datenerhebung bedurfte es daher jeweils einer wirksamen Einwilligung der Betroffenen oder einer gesetzlichen Grundlage. Grundsätzlich sieht der TLfDI die Verwendung von Einwilligungserklärungen für Mietinteressenten in Formularen zur Selbstauskunft nicht als richtiges Mittel zur Datenerhebung an. Eine wirksame Einwilligung erfordert nach § 4a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Häufig wird dem

Mietinteressenten bei Mieterselbstauskünften suggeriert, dass er bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht habe. Wird aber der Abschluss des Mietvertrages von der Erhebung bestimmter Angaben beim Mietinteressenten abhängig gemacht, entfällt gerade diese vermeintliche Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommen kann. Deshalb war die von der Haus- und Immobilienverwaltung mit den Mieterauskünften angestrebte Einwilligung für die Mietinteressenten in der Mieterselbstauskunft datenschutzrechtlich nicht zulässig.

Wegen dieser fehlenden Dispositionsmöglichkeit auf Seite des potentiellen Mieters richtet sich die Zulässigkeit der Erhebung einer Selbstauskunft im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG. Hiernach ist das Erheben personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis zum künftigen Vermieter. Aber auch hier sind Fallstricke versteckt. Es ist immer auf die Erforderlichkeit des einzelnen, jeweils abgerufenen Datums abzustellen. Im vorliegenden Fall stellte der TLfDI fest, dass die Haus- und Immobilienverwaltung in der verwendeten Mieterselbstauskunft Daten, wie zum Beispiel das Geburtsdatum, erfragte, die zu Beginn der Mietvertragsverhandlungen (noch) nicht erforderlich und die teilweise auch in den weiteren Stadien der Vertragsanbahnung unzulässig waren, da sie das Mietverhältnis nicht betrafen.

Der TLfDI teilte der Haus- und Immobilienverwaltung mit, dass bezüglich der Datenerhebung zwischen drei Zeitpunkten differenziert werden muss: 1. dem Besichtigungstermin, 2. der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und 3. der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten. Daher empfiehlt der TLfDI zur formularmäßigen Abfrage von Mietdaten ein dreistufiges Verfahren. (s. Tätigkeitsbericht „Keine vollständige Mieterselbstauskunft bei Besichtigungsterminen“ Beitrag 2.28).

Die Haus- und Immobilienverwaltung korrigierte das Formular zur Mieterselbstauskunft entsprechend den Hinweisen des TLfDI und passte den Zeitpunkt der Abfrage an die Forderungen des TLfDI an. Somit konnte der TLfDI das Verfahren erfolgreich abschließen.

Bezüglich der datenschutzzulässigen Datenerhebung von Haus- und Immobilienverwaltungen muss zwischen drei Zeitpunkten differenziert werden: 1. dem Besichtigungstermin, 2. der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und 3. der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten. Daher empfiehlt der TLfDI zur formularmäßigen Abfrage von Mieterdaten ein dreistufiges Verfahren.

2.30 Abrechnungsverfahren und Auskunftsverlangen im Bestattungsunternehmen

Ein Beschwerdeführer wandte sich mit einem Auskunftsverlangen nach § 34 Bundesdatenschutzgesetz (BDSG) an ein Bestattungsunternehmen. Er wollte in Erfahrung bringen, welche Daten das Unternehmen von ihm gespeichert und woher es seine personenbezogenen Daten hatte. Weiterhin wollte er wissen, ob und an wen diese Daten weitergegeben wurden sowie den Zweck der Speicherung seiner Daten mitgeteilt bekommen. Anlass des Auskunftsersuchens war eine durch das Bestattungsunternehmen an den Beschwerdeführer übersandte anteilige Rechnung über die Bestattungskosten für dessen verstorbene Mutter, zu der er keinen Kontakt mehr pflegte. Das Ordnungsamt hatte ursprünglich eine Tochter der Verstorbenen angeschrieben und auf die Bestattungspflicht hingewiesen. Diese nahm sich zwar der Organisation der Bestattung an, teilte jedoch dem Bestattungsunternehmen auch die Adresse ihres Bruders, der gleichzeitig das älteste Kind der Verstorbenen war, mit. Nach § 18 Abs. 1 Thüringer Bestattungsgesetz (ThürBestG) ist das älteste Kind der Verstorbenen bestattungspflichtig und muss die Kosten dafür tragen. Daher sah sich die ursprünglich angeschriebene Tochter nicht in der Pflicht. Das Bestattungsunternehmen schlug deshalb vermittelnd vor, den Gesamtbetrag unter den zurückgebliebenen Geschwistern und dem Lebenspartner der Verstorbenen aufzuteilen. Daraufhin erhielt der Beschwerdeführer das o. g. Schreiben des Bestattungsun-

ternehmens, welches den Anlass des Auskunftsverlangens gemäß § 34 BDSG darstellte.
Der TLfDI konnte aufklären, dass das Bestattungsunternehmen die personenbezogenen Daten des Beschwerdeführers nicht an Dritte übermittelt hatte. Es wurde festgestellt, dass zwar die Rechnungslegung und -versendung direkt durch das Bestattungsunternehmen erfolgte, Zahlungsempfänger jedoch ein Abrechnungsunternehmen war. Zu Abrechnungszwecken wurde jeweils die Rechnung an das Abrechnungsunternehmen per Fax übermittelt. Diese Gesamtrechnung wurde jedoch auf die ursprünglich angeschriebene Schwester ausgestellt. Die übrigen Geschwister wurden durch das Bestattungsunternehmen nur mit einem einfachen Brief aufgefordert, ihren Anteil zu begleichen. Dem Bestattungsunternehmen wurde jedoch ausführlich dargelegt, dass der Forderungseinzug für das Bestattungsunternehmen durch ein Abrechnungsunternehmen dem Bestattungsunternehmen zugerechnet werde und nur im Rahmen einer Auftragsdatenverarbeitung i. S. v. § 11 BDSG zulässig sei. Es wurde verdeutlicht, dass das Bestattungsunternehmen die verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG war, ein Auftragsdatenverarbeitungsvertrag erforderlich gewesen wäre und dieser dem TLfDI vorzulegen war.

Zwar wurden alle Auskunftsersuchen des TLfDI und des Beschwerdeführers anstandslos beantwortet, jedoch legte das Unternehmen trotz Aufforderung bislang den angeforderten Vertrag über die Auftragsdatenverarbeitung nicht vor. Der TLfDI prüft die Möglichkeit des Erlasses eines Anordnungsbescheides und die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 1 Nr. 2b BDSG.

Zweck eines Auskunftsverlangens nach § 34 Abs. 1 BDSG ist es zu erfahren, welche personenbezogenen Daten ein Unternehmen gespeichert hat, und woher es diese Daten hat sowie ob und an wen personenbezogene Daten weitergegeben wurden. Sobald ein Unternehmen eigene Aufgaben, die einen Umgang mit personenbezogenen Daten erfordern, an ein anderes Unternehmen outsourced, ist ein Vertrag über die Auftragsdatenverarbeitung nach § 11 BDSG zu schließen. Wer einen Auftragsdatenverarbeitungsvertrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt, kann sich einem Bußgeldverfahren nach § 43 Abs. 1 Nr. 2b BDSG aussetzen.

2.31 TLfDI als Partnervermittlung – bei Vertragsabschluss immer auch das Kleingedruckte lesen!

Eine Bürgerin, die mit einem Partnervermittlungsinstitut einen Vertrag über die Anbahnung von Kontakten über eine Kontaktbörse abgeschlossen hatte, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Unterstützung wegen der Nichterfüllung von vertraglich zugesicherten Leistungen. Der TLfDI stellte zunächst fest, dass die Bürgerin sich mit ihrer Unterschrift unter dem Vermittlungsvertrag damit einverstanden erklärt hatte, dass die von ihr bekannt gegebenen Daten registriert und an Dritte, die an einer Kontaktaufnahme mit ihr interessiert sind, weitergegeben werden. Im „Kleingedruckten“ stand auch, dass über die Richtigkeit der persönlichen Daten der Partnersuchenden sowie das Zustandekommen eines Kontaktes mit einer bestimmten Person von der Kontaktbörse leider keine Gewähr übernommen werden könne. Hierauf wies der TLfDI die Beschwerdeführerin hin. Anhaltspunkte für einen datenschutzrechtlichen Verstoß waren aus dem Vorbringen der Beschwerdeführerin nicht zu entnehmen, denn die Daten der Beschwerdeführerin waren von dem Unternehmen offensichtlich auf vertraglicher Grundlage verarbeitet und genutzt worden. Für die Prüfung, ob das Unternehmen andere Leistungen aus dem Vertrag nicht erfüllt hatte, verwies der TLfDI die Bürgerin an die Verbraucherzentrale.

Der zulässige Umgang mit personenbezogenen Daten durch ein Unternehmen für die Anbahnung von Kontakten ergibt sich grundsätzlich aus den vertraglichen Klauseln. Eine Zuständigkeit des TLfDI für die Prüfung, ob das Unternehmen vertraglich zugesicherte Leistungen erfüllt hat, die keinen Bezug zu einem datenschutzrechtlich relevanten Problem haben, ist nicht gegeben.

2.32 Moderne Fernseh-Computer im Wohnzimmer: Smart-TV

Moderne Fernsehgeräte (Smart-TV) können heutzutage nicht nur wie herkömmliche Fernseher genutzt werden, sie bieten zudem u.a. auch die Möglichkeit, Internetseiten oder Beiträge aus Mediatheken aufzurufen. Durch diese Online-Verbindung entsteht allerdings nun ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Somit ist es möglich, das individu-

elle Nutzungsverhalten zu erfassen, auszuwerten und ggf. Angebote entsprechend anzupassen.
Um diese neue Technologie datenschutzrechtlich bewerten und begleiten zu können, wurde seitens der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) eine Unterarbeitsgruppe (UAG) zum genannten Thema unter der Federführung des Bayrischen Landesamtes für Datenschutzaufsicht (BayLDA) gegründet.
Der Düsseldorfer Kreis und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten forderten zudem in einem gemeinsamen Positionspapier im Mai 2014 die Möglichkeit, Fernsehangebote auch anonym nutzen zu können, entsprechend dem Telemediengesetz bei der Bildung von Nutzerprofilen die vorhergehende Einwilligung der Betroffenen einzuholen, die Internetverbindung oder die Nutzung von Diensten erst nach aktiver Freischaltung durch den Benutzer selbst zu aktivieren und die Geräte vor dem Zugriff unbefugter Dritter zu schützen (siehe Anlage 6).
Im September 2014 lud dann der Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI) auf die IFA zu einem Gespräch mit den führenden Smart-TV-Geräteherstellern. An diesem Gespräch nahm auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) teil. Auf der Grundlage dieses Gespräches erarbeitete das BayLDA einen Fragenkatalog zur Smart-TV-Prüfung. Ziel dabei war es, zu klären, welche Datenflüsse vorhanden sind, wohin die Datenübermittlung erfolgt und welche Einstellmöglichkeiten die Geräte für die Nutzer bieten. Ende 2014 wurden in Absprache mit und in Amtshilfe vom BayLDA 13 aktuelle Smart-TVs einer technischen Prüfung unterzogen. Die verschiedensten Gerätehersteller hatten dabei alle ihren Sitz bzw. zumindest eine Niederlassung in Deutschland. Nach Angaben des BayLDA betrug dabei die Marktabdeckung der Gerätehersteller ca. 90 %, sodass im Ergebnis von einem repräsentativen Einblick in die Funktionalitäten der Geräte ausgegangen werden kann.
Das Ergebnis dieser Prüfung überraschte insofern, da nicht nur Informationen über das Umschalten auf einen anderen Sender und das Aufnehmen von Sendungen zum Teil an den Gerätehersteller übermittelt werden, sondern bei vier geprüften Geräten auch die Tatsache der Nutzung von USB-Sticks registriert und an den Hersteller weitergeleitet wurde. Auch wenn wohl derzeit keine Musiktitel oder Namen von Videodateien oder Bilddateien mit übertragen werden,

so könnte dies doch bei einigen Nutzern ein mulmiges Bauchgefühl entwickeln. Dies zu Recht, denn solche Funktionalitäten lassen sich per Softwareupdate beim Fernseher schnell unbemerkt erweitern bzw., wenn noch nicht vorhanden, nachinstallieren.

Den Gesamtüberblick der Prüf-Ergebnisse können Sie übrigens einsehen unter:

https://www.lda.bayern.de/lda/datenschutzaufCsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20DrucD.pdf

Angemerkt sei allerdings, dass in die Prüfung keine Apps einbezogen werden konnten, die der Nutzer selbst aus irgendwelchen App-Stores noch auf sein Fernsehgerät lädt.

Im Nachgang dieser Prüfung wurde u. a. deshalb vom Düsseldorfer Kreis eine „Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste“ erarbeitet. Sie richtet sich an die Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Geräteherstellen, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und Anbieter von HbbTV-Angeboten. HbbTV ist ein Standard und die Abkürzung für Hybrid broadcasting broadband TV. Es bedeutet, dass sowohl das Rundfunksignal (broadcasting) als auch das Breitbandinternet (broadband) genutzt werden, um zahlreiche Zusatzinformationen am Fernseher anzubieten. So werden z. B. Zusatzinformationen zum TV-Programm durch die Sender zur Verfügung gestellt oder ein Zugriff auf Mediatheken oder soziale Netzwerke ermöglicht.

Die Orientierungshilfe gibt auch einen Überblick über die datenschutzrechtliche Bewertung durch die zuständigen Aufsichtsbehörden.

Diese aktuelle Orientierungshilfe finden Sie auf der Webseite des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) unter:
https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_smart_tv_v1.0.pdf

Unabhängig von der Prüfung und der Orientierungshilfe wurde der TLfDI 2015 von der Thüringer Landesmedienanstalt zu diesem Thema in deren Technik-Ausschuss eingeladen. Ziel der Landesmedienanstalt war es zu erfahren, welche datenschutzrechtlichen Pflichten sich für die Smart-TV-Dienste-Anbieter ergeben und welche datenschutzrechtlichen Risiken es für Nutzer von Smart-TV gibt.
Da das Gespräch als sehr konstruktiv angesehen wurde, äußerten die Teilnehmer den Wunsch, zukünftig den TLfDI öfter beratend hinzuzuziehen.

Die „Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste“ richtet sich an die Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter und Anbieter von Empfehlungsdiensten. Die Orientierungshilfe gibt auch einen Überblick über die datenschutzrechtliche Bewertung durch die jeweilig zuständigen Aufsichtsbehörden.

2.33 Ein Virus kommt selten allein – Schutz von Firmennetzwerken

Ab und zu kommt es vor, dass Computer von Firmennetzen von einer Schadsoftware befallen werden. Dies kann z. B. durch Installation von mit Viren verseuchter Software oder manipulierten Mailanhängen geschehen. Im vorliegenden Fall ist dies einer Firma in Thüringen passiert, indem eine per Mail an sie verschickte gefälschte Telefonrechnung einschließlich ihrer Anlagen geöffnet und sogar mehrfach weitergeleitet wurde. Durch das Öffnen des Anhangs installierten sich die Viren auf dem Computer. Zum Zeitpunkt des Befalls war sowohl eine Firewall als auch ein Virenscanner aktiv, und dennoch konnte ein Virus gleich mehrere Systeme infizieren. Die Viren waren zu aktuell, um von den Virenscannern erkannt zu werden.
Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) muss solch ein Vorfall gemäß § 42a Bundesdatenschutzgesetz (BDSG) mitgeteilt werden, wenn dabei unrechtmäßig personenbezogene Daten aus dem Katalog des § 42a BDSG übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen zu

erwarten ist. Gleichzeitig sind auch die Betroffenen selbst unverzüglich zu informieren.
Nach Angaben der Firma waren im vorliegenden Fall die Online-Banking-Daten des Unternehmens ausgespäht worden. Weiterhin wurde vermutet, dass auch die E-Mail-Adressen der betroffenen Mitarbeiter ausgelesen wurden. Welche Daten sonst noch abhandengekommen waren, konnte nicht festgestellt werden.
Dieser Fall ist besonders deshalb interessant, weil es durch eine Reihe von Zufällen überhaupt erst so weit kommen konnte. Der erste Zufall war, dass der Virenscanner des E-Mail-Posteinganges den Virus nicht erkennen konnte, da der Virus zu neu war und der Scanner die aktuelle Virensignatur noch nicht erkannt hat. Aus datenschutzrechtlicher Sicht ist es deshalb wichtig, mehrfach am Tag (mindestens jede Stunde) den Virenscanner zu aktualisieren. Der zweite unglückliche Zufall war, dass die Mail geöffnet wurde und drittens, dass sie dann auch noch an verschiedene Mitarbeiter weitergeleitet wurde. Auf jedem Computer begann die Schadsoftware dann, andere Schädlinge herunterzuladen und ebenfalls auf dem jeweiligen Computer zu installieren. Und – letzter Zufall – so kam ein so genannter Trojaner zum Ausspionieren von Bankdaten auf den Rechner, der für den Zahlungsverkehr des Unternehmens genutzt wurde. Schädlinge gab es nun reichlich; darunter waren solche zum Versenden von Massenmails, zur Überwachung von Tastatureingaben, zum Deaktivieren des Virenscanners, zum Umleiten von Webseitenaufrufen und zum externen Zugriff auf den Rechner. Einige davon wurden vom Virenscanner in Quarantäne versetzt und wurden nicht wirksam. Von einer Computerfirma wurden anschließend alle Rechner des Unternehmens auf Schädlingsbefall untersucht. Die betroffenen Rechner wurden anschließend gesäubert und die Virenscanner neu installiert.
Der TLfDI gab zusätzlich noch Hinweise zur sicherheitstechnischen Verbesserung der IT-Systeme: zum Beispiel ein zentraler Virenscanner für den E-Mail-Server und die zusätzliche E-Mail-Prüfung in der Firewall. Außerdem hat der TLfDI empfohlen, zusätzlich Einstellungen beim Proxy-Server zu prüfen.

Für den Fall, dass personenbezogene Daten nach § 42a BDSG Dritten unrechtmäßig zur Kenntnis gelangt sind, ist für Unternehmen in Thüringen der TLfDI zu informieren. Trotz Virenschutz und Firewall kann es dennoch vorkommen, dass ein Virus auf einen Compu-

ter gelangt. Man sollte als Nutzer immer wachsam und misstrauisch sein. Eine Garantie für absolute Sicherheit gibt es auch durch gängige Sicherheitsmaßnahmen nicht. Sie helfen aber, das Risiko zu vermindern.

2.34 Müllcontainer statt Briefkasten

Ein Mitarbeiter eines Versorgungsbetriebs staunte nicht schlecht, als er beim Blick in einen Müllcontainer feststellte, dass in diesem fast 200 an konkrete Personen adressierte und frankierte Briefe lagen. Die Briefe wurden dem Behälter entnommen und von der Betriebsleitung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) übergeben. Der TLfDI konnte nicht ausschließen, dass der Vorfall strafrechtliche Relevanz besaß, etwa weil die Briefe entweder einem Postzusteller gestohlen worden waren oder ein solcher sich der Briefe unter Verstoß gegen § 39 Abs. 3 des Postgesetzes entledigt hatte. Da der TLfDI selbst keine Zuständigkeit für die Verfolgung von Straftaten hat, gab er die Angelegenheit einschließlich der im Müllcontainer aufgefundenen Briefe an die Staatsanwaltschaft ab.

Für die Verfolgung von Straftaten, auch solche, die im Zusammenhang mit datenschutzrechtlich relevanten Sachverhalten stehen, ist nicht der TLfDI als datenschutzrechtliche Aufsichtsbehörde für den nicht-öffentlichen Bereich, sondern die Staatsanwaltschaft zuständig. Nach § 44 Bundesdatenschutzgesetz ist unter anderem der TLfDI berechtigt, einen Strafantrag auf Verfolgung der Tat zu stellen.

2.35 Nicht immer ist der TLfDI zuständig

Von besorgten Bürgern erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum fast 90 Anfragen und Beschwerden, die nicht in den Zuständigkeitsbereich TLfDI fielen. Denn der TLfDI kontrolliert gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Die örtliche Zuständigkeit richtet sich grundsätzlich nach dem Sitz der für die Datenverarbeitung ver-

antwortlichen Stelle bzw. nach dem Ort einer Betriebsstätte. Bei eingegangener Briefpost wurde der Beschwerdeführer über die Nichtzuständigkeit des TLfDI informiert und angefragt, ob die Anfrage vom TLfDI an die zuständige Stelle gesandt werden solle. Nur mit dem Einverständnis des Beschwerdeführers wurden diese Schreiben weitergeleitet. Bei Posteingängen per E-Mail wurde den Beschwerdeführern die Adresse der zuständigen Aufsichtsbehörde genannt, damit diese ihre Beschwerde an diese Stelle weiterleiten konnten.

Beispiele für die Unzuständigkeit des TLfDI

Nicht zuständig ist der TLfDI für die Datenverarbeitung bei Unternehmen aus dem Bereich der Telekommunikation (Telefonanbieter). Für die Datenschutzkontrolle ist dort in jedem Fall die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) mit Sitz in 53117 Bonn, Husarenstraße 30, (E-Mail: poststelle@bfdi.bund.de) zuständig, unabhängig davon, wo das Unternehmen seinen Sitz hat (§ 115 Abs. 4 Telekommunikationsgesetz).
Die Jobcenter gehören in der großen Mehrzahl zur Bundesagentur für Arbeit. Seit dem 1. Januar 2011 liegt die datenschutzrechtliche Zuständigkeit für diese Jobcenter ebenfalls bei der BfDI. Außerdem besteht die Möglichkeit, dass die Kommunen Jobcenter in eigener Zuständigkeit betreiben, so genannte Optionskommunen. Optionskommunen sind in Thüringen nur die Stadt Jena und die Landkreise Eichsfeld, Greiz und Schmalkalden-Meiningen, hierfür liegt eine Zuständigkeit des TLfDI vor.
Der Bereich des Rundfunks (Radio, Fernsehen) ist aus verfassungsrechtlichen Gründen aus der Kontrollbefugnis der Landesdatenschutzbeauftragten ausgenommen. Wegen der Unabhängigkeit und Staatsferne des öffentlich-rechtlichen Rundfunks gibt es Besonderheiten bei der Datenschutzkontrolle. Sämtliche öffentlich-rechtliche Rundfunkanstalten haben einen eigenen internen Rundfunkdatenschutzbeauftragten, der die Datenschutzkontrolle durch die unabhängigen Landesdatenschutzbeauftragten ersetzt. Da Thüringen im Sendebereich des Mitteldeutschen Rundfunks liegt, müsste ein Beschwerdeführer sich zuständigkeitshalber an den Datenschutzbeauftragten des Mitteldeutschen Rundfunks, Kantstraße 71–73 in 04275 Leipzig, E-Mail: datenschutz@mdr.de, Telefon: 0341/300-7732 wenden. Es besteht aber auch die Möglichkeit, sich

direkt an die Datenschutzbeauftragte des ARD ZDF Deutschlandradio Beitragsservice unter der Adresse: ARD ZDF Deutschlandradio, Beitragsservice, Datenschutzbeauftragte, Freimersdorfer Weg 6 in 50829 Köln, zu wenden.
Für die Kontrolle der Verarbeitung personenbezogener Daten durch kirchliche Stellen ist durch das verfassungsrechtlich garantierte Selbstbestimmungsrecht von Religionsgemeinschaften das BDSG dort nicht anwendbar. Die Evangelische Kirche in Deutschland und die Bistümer der Katholischen Kirche in Deutschland haben eigene Datenschutzvorschriften erlassen (die evangelische Kirche beispielsweise das Datenschutzgesetz der Evangelischen Kirche in Deutschland [DSG-EKD]) und sie haben auch eigene Datenschutzbeauftragte. Für die Evangelische Kirche in Thüringen ist der Datenschutzbeauftragte des Diakonischen Werkes Evangelischer Kirchen in Mitteldeutschland e.V., Ingenieurbüro für Datenschutz und Datensicherheit, Dipl.-Ing. P.-G. Große, Albrecht-Thaer-Straße 5 in 09117 Chemnitz zuständig. Anfragen im Bereich der katholischen Kirche können an das Bistum Erfurt, Justiziarin, Herrmannsplatz 9 in 99084 Erfurt gerichtet werden.

Der TLfDI kontrolliert gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Die örtliche Zuständigkeit richtet sich grundsätzlich nach dem Sitz der für die Datenverarbeitung verantwortlichen Stelle bzw. nach dem Ort einer Betriebsstätte.

2.36 Datentonnen – dramatische Beschwerde mit nichts dahinter

Im Berichtszeitraum wandte sich ein Beschwerdeführer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte in dramatischen Worten mit, dass ein Rechtsanwalt Datentonnen in einem Treppenhaus lagern würde, die so voll wären, dass jedermann durch den Einwurf Unterlagen herausziehen könne.
Zustände, die eine sofortige Kontrolle vor Ort unausweichlich machten. Vor Ort stellte der Mitarbeiter des TLfDI allerdings fest, dass die Datencontainer nicht zur im Hause ansässigen Rechtsanwalts-

kanzlei gehörten, sondern zu einem vollkommen anderen Unternehmen. Noch dazu waren die Datentonnen vorbildlich gesichert. Zwischen Deckel und Inhalt war jeweils ein großer Karton als „Zwischendeckel“ eingelegt, der verhinderte, dass man durch den Einwurf an irgendwelche Dokumente kam. Selbstverständlich waren die Tonnen abgeschlossen. Im Laufe der Kontrolle stellte sich letztlich heraus, dass die Tonnen noch dazu überhaupt nicht mit personenbezogenen Daten gefüllt waren, sondern das Unternehmen lediglich alte Werbeflyer weggeworfen hatte, die nicht im Müll „herumfliegen“ sollten. Unterm Strich war an den Vorwürfen folglich überhaupt nichts dran.
Der TLfDI geht im Rahmen seiner Möglichkeiten jedem Vorwurf nach. Wird der TLfDI allerdings falsch informiert, möglicherweise um dazu gebracht zu werden, ein unliebsames Unternehmen zu kontrollieren, obwohl die Vorwürfe nicht zutreffen, hat der TLfDI, so hat es der Gesetzgeber geregelt, dem gegenüber die Gebühren und Auslagen festzusetzen, der diese verursacht hat, § 42 Abs. 4 Satz 3 Thüringer Datenschutzgesetz. Einzige Ausnahme sind hier Billigkeitserwägungen.
So stellte sich im Übrigen auch dieser Fall dar. Die Person, die die Vorwürfe erhoben hatte, befand sich in psychologischer Behandlung, weswegen davon abgesehen wurde, ihr die Kosten für die Kontrolle aufzuerlegen.

Die Kosten einer Kontrolle trägt die kontrollierte Stelle nur, wenn datenschutzrechtliche Mängel festgestellt werden können. Stellen sich die Vorwürfe jedoch als „an den Haaren herbeigezogen“ heraus, wird der TLfDI prüfen, ob die Kosten dem Hinweisgeber auferlegt werden. Dabei kann es sich schnell um mehrere hundert Euro handeln.

2.37 Taxifahrt zum Staatsanwalt – Einsatz von GPS bei Taxis

Gleich mit mehreren schwerwiegenden Beschwerden gegen eine Taxizentrale wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Nach Ausführungen des Beschwerdeführers gibt es einen Mitschnitt der Bestelltelefonate der Kunden. Zusätzlich erfolge ein sogenanntes Tracking der Taxis, also eine umfassende Kontrolle über die Fahrstrecke und Fahrtunterbrechungen. Darüber hinaus habe die Taxi-

zentrale alle angeschlossenen Taxifahrer angewiesen, sich den Namen und die angezeigte Telefonnummer des Bestellers zu notieren und diese Angaben dann der dazugehörigen Adresse bei Abholung von der Haustür zuzuordnen. Bei einem erneuten Bestellanruf könnten somit automatisch der Name, die Adresse und die Telefonnummer des Bestellers auf dem Display des Taxameters erscheinen. Nach Aussage des Beschwerdeführers erfolge diese Vorgehensweise ohne Wissen und Einwilligung der Bestellkunden. Die Taxizentrale führte gegenüber dem TLfDI aus, dass sie selbst als Vermittlungszentrale keine eigenen Taxen betreibe, vielmehr seien verschiedene Taxibetriebe als Vertrags- bzw. Anschlusspartner der Taxizentrale angeschlossen. Mit diesen schließe sie so genannte Anschlussverträge, nach welchen über eine zentrale Rufnummer Bestellanrufe an die einzelnen Taxis vermittelt werden. Dafür erhebe die Taxizentrale ein Vermittlungsentgelt. Eine datenschutzrechtliche Vereinbarung zwischen den angeschlossenen Taxiunternehmen und der Zentrale würde nicht bestehen. Die Verbindung zwischen dem anrufenden Kunden und dem einzelnen Taxifahrer würde automatisch hergestellt werden. Dabei sei es vollkommen irrelevant, welche Telefonnummer der Kunde anrufe. Das Stadtgebiet sei in verschiedene Sektoren aufgeteilt. Die Position der einzelnen Taxen würde man via GPS in den Smartphones ermitteln. Diese Smartphones stehen allerdings im Eigentum der jeweiligen angeschlossenen Taxiunternehmen. Dann erfolge eine automatische Zuordnung des GPS-Signals auf den Server der Taxizentrale und zu einem der Sektoren.
Daraufhin forderte der TLfDI die Taxizentrale zur Vorlage eines solchen Muster-Vermittlungsvertrages mit den jeweiligen Anschlusspartnern auf. Bisher liegt dem TLfDI noch kein solches Vertragsmuster zur Überprüfung vor.
Für den TLfDI steht im Raum zu prüfen und zu bewerten, ob die Überwachung mittels des GPS-Trackingsystems der Taxizentrale und deren angeschlossenen Taxiunternehmen – dies wiederum bezogen auf die einzelnen Taxifahrer – zulässig ist. Nach § 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) kann das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten der Taxifahrer oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig sein, soweit es zur Wahrung berechtigter Interessen der Taxizentrale, als verantwortliche Stelle, erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Taxifahrer am Ausschluss der Verarbeitung oder Nut-

zung überwiegt. Durch GPS ist es möglich, den Aufenthaltsort von Personen in ihren Fahrzeugen permanent zu überwachen. Prinzipiell werden zwar nur die Fahrzeuge geortet. Aufgrund der Zuordnung einzelner Fahrzeuge zu den jeweiligen Taxifahrern entsteht jedoch ein Personenbezug, sodass es sich bei Standortdaten von GPS-Geräten um personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG handelt.

Nach dem datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG): „Alles, was nicht erlaubt ist, ist verboten“, ist der Einsatz von GPS-Systemen nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder eine wirksame Einwilligung des Betroffenen gemäß § 4a BDSG vorliegt. Im Arbeitsverhältnis lässt sich die grundsätzlich in § 32 Abs. 1 BDSG geregelte Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten nur in engen Grenzen auf Einwilligungen der Beschäftigten stützen, denn aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber liegt eine die Einwilligung voraussetzende Freiwilligkeit der Entscheidung in aller Regel nicht vor. Im vorliegenden Fall handelt es sich aber nach derzeitiger Aktenlage und Aussage der Taxizentrale gerade nicht um Abhängigkeitsverhältnisse, sondern um selbstständige Anschlusspartner. Der § 32 Abs. 1 BDSG wäre hier somit nicht einschlägig.

Im Einzelnen kommt es auf den Zweck der Datenverarbeitung, die technischen Möglichkeiten des Systems und dessen tatsächlichen Gebrauch an. Eine zulässige Datenerhebung mittels Ortungstechnik erfordert eine konkrete Festlegung der Zwecke, für die die Daten verarbeitet oder genutzt werden sollen (§ 28 Abs. 1 Satz 2 BDSG). Hierfür genügt ein pauschaler Hinweis auf die Erhebung gesetzlich vorgeschriebener Daten nicht. Erst wenn die Zwecke der Erfassung bestimmter Daten konkretisiert sind, lässt sich die Erforderlichkeit im Einzelnen beurteilen.

So wäre es datenschutzrechtlich unproblematisch, wenn die Ortung durch das System technisch etwa erst nach einem Kfz-Diebstahl einsetzen würde. Beispielsweise können Speditionen zur Warenverfolgung ihren Fuhrpark orten. Solche der Ortung von Gegenständen dienende Zwecke, die offensichtlich im berechtigten Interesse des Unternehmens liegen, sind grundsätzlich zulässig. Soweit dabei zugleich Daten des Fahrpersonals gespeichert werden, sind aber weitere Regelungen über den Umgang mit diesen Daten zu beachten. Auswertungsfunktionalitäten, die nur der allgemeinen persönlichen

Überwachung dienen können (wie etwa Geschwindigkeitsaufzeichnungen, Dauer von Fahrtunterbrechungen), sind regelmäßig technisch zu unterbinden. Ein System zum Beispiel, das über eine Alarmierungsfunktion verfügt, die darüber informiert, wenn eine definierte Zone verlassen oder sich zu lange in einer solchen aufhalten wird, würde einen permanenten Kontrolldruck erzeugen. Es ist deswegen nicht zulässig.
Das Verfahren ist aber bisher noch nicht abgeschlossen, über den Ausgang des Verfahrens wird der TLfDI im nächsten Tätigkeitsbericht informieren.
Da auch die geschilderte Verfahrensweise, der Mitschnitt von Bestelltelefonaten der Kunden, einen strafrechtlich relevanten Sachverhalt im Sinne des § 201 Strafgesetzbuch (StGB) enthielt, wurde das Verfahren teilweise an die Staatsanwaltschaft mit der Bitte um Verfolgung der Angelegenheit in dortiger Zuständigkeit abgegeben. Über den Ausgang des Verfahrens der Staatsanwaltschaft hat der TLfDI bisher keine Kenntnis.

Eine zulässige Datenerhebung mittels Ortungstechnik erfordert eine konkrete Festlegung der Zwecke, für die die Daten verarbeitet oder genutzt werden sollen (§ 28 Abs. 1 Satz 2 BDSG). Erst wenn die Zwecke der Erfassung bestimmter Daten konkretisiert sind, lässt sich die Erforderlichkeit im Einzelnen beurteilen. Soweit bei der Ortung zugleich Daten des Fahrpersonals gespeichert werden, sind aber weitere Regelungen über den Umgang mit diesen Daten zu beachten.

2.38 Datenschutz im Reich der Toten? Welche Daten dürfen Genealogen nutzen?

Genealogen beschäftigen sich mit menschlichen Verwandtschaftsbeziehungen und ihrer Darstellung. Je weiter die Darstellungen von Verwandtschaftsbeziehungen zurückreichen, umso höher ist die Wahrscheinlichkeit, dass es sich um verstorbene Verwandte handelt, während bei der Darstellung der aktuellen Verwandtschaftsverhältnisse von lebenden Personen auszugehen ist. Ein Genealoge wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Auskunft, wie mit Forschungsergebnissen einzelner Genealogen umgegangen werden kann, die ihre entweder in schriftlicher oder aber in elektronischer Form festgehaltenen Verwandtschaftsbeziehungen nach ihrem Tod

einer genealogischen Gesellschaft oder einem genealogischen Verein vermachen. Insbesondere bezog sich die Anfrage auf Datensätze von noch lebenden Personen, die etwa neben dem Namen der Person auch Informationen zu Geburt, Taufe, Firmung, Konfirmation, Jugendweihe, Beruf, Wohnadresse, E-Mail, Geschwistern, Eltern usw. umfassen. Der TLfDI teilte dem Genealogen mit, dass bei der rein privaten Beschäftigung mit genealogischen Daten noch von einer persönlichen oder familiären Tätigkeit im Sinne von § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetzes (BDSG) ausgegangen werden kann und das BDSG keine Anwendung findet. Allerdings beurteilt sich bereits die Übermittlung von personenbezogenen Daten mit einer Verwandtschaftsdarstellung an einen Dritten, etwa an einen Verein, nach den Vorschriften des BDSG. Dies gilt auch dann, wenn der Genealoge seine zunächst rein private Beschäftigung mit Verwandtschaftsverhältnissen im Internet veröffentlicht. Hierin liegt sogar die weitreichendste Form einer Veröffentlichung. Gemäß § 4 Abs. 1 BDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Da weder die Vorschriften des BDSG, noch andere spezial-gesetzliche Bestimmungen die Veröffentlichung von genealogischen personenbezogenen Daten erlauben, ist die Übermittlung von Daten lebender Personen nur mit Einwilligung der Betroffenen zulässig.
Bei der Übermittlung von Daten bereits verstorbener Personen fehlt im BDSG eine ausdrückliche Regelung Hier ist zu prüfen, ob das postmortale Persönlichkeitsrecht, welches sich aus der Menschenwürde (Artikel 1 Abs. 1 Grundgesetz) ergibt, durch die Übermittlung verletzt wird. Darüber hinaus können bestimmte Daten eines Verstorbenen auch zugleich Angaben über eine lebende Person sein, zum Beispiel wenn der Verstorbene an einer Erbkrankheit litt oder einen nicht sozialadäquaten Beruf ausübte usw. In diesen Fällen muss ebenfalls eine Einwilligung bei den betroffenen Nachkommen eingeholt werden. Im Ergebnis des Kontakts mit dem Genealogen hat der TLfDI auf dem Deutschen Genealogentag am 3./4. Oktober 2015 in Gotha vor zahlreichen Genealogen einen Vortrag zu Genealogie und Datenschutz gehalten.

Bei der genealogischen Forschung zu rein privaten oder familiären Zwecken finden die Regelungen des BDSG keine Anwendung. Sobald eine Veröffentlichung von Ergebnissen dieser Forschung er-

folgt, gelten aber die Regelungen des BDSG. Auch die Veröffentlichung von Daten Verstorbener kann in Einzelfällen nur auf der Grundlage einer Einwilligung noch lebender Nachkommen zulässig sein. Zu beachten ist bei Verstorbenen auch das postmortale Persönlichkeitsrecht. Dieses ist aber nicht Gegenstand der Regelungen der Datenschutzrechte.

2.39 Auskunftserteilung eines Unternehmens: Besser spät als nie

Seit November 2014 beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Fall einer unterbliebenen Auskunftserteilung eines Unternehmens gegenüber dem Bürger. Anlass des Auskunftsersuchens war eine vorausgehende Bestellung in einem Online-Shop über ein Verkaufsportal. Der Bürger wandte sich mit einem Auskunftsersuchen an das Unternehmen und bat um Mitteilung über die zu seiner Person gespeicherten Daten und die Herkunft dieser. Weiterhin erstreckte sich das Auskunftsersuchen auf die Angabe der Empfänger, an die Daten weitergegeben werden, soweit dies der Fall ist, und den Zweck der Speicherung. Das Unternehmen hat eine Pflicht zur Auskunftserteilung nach § 34 Bundesdatenschutzgesetz (BDSG). Da der Beschwerdeführer auf sein Auskunftsersuchen im Rahmen der gesetzten Frist keine Antwort erhalten hat, wandte er sich an den TLfDI. Eine Auskunftserteilung erfolgt bereits nicht rechtzeitig, wenn die vom Bürger gesetzte, angemessene Frist verstrichen ist. Von einer angemessenen Frist ist, wenn keine besonderen Umstände hinzukommen, in der Regel bei einem Zeitraum von zwei Wochen auszugehen.
In diesem Fall wurde eine Frist von weniger als zwei Wochen gesetzt. Daher trat der TLfDI an das Unternehmen heran und wies unter angemessener Fristsetzung auf die Rechtslage hin. Telefonisch sicherte das Unternehmen nach kurzer Zeit zu, das Auskunftsersuchen des Bürgers zu beantworten. Nachdem eine Beantwortung auch nach ca. zwei Monaten noch nicht erfolgte, leitete der TLfDI ein Bußgeldverfahren gegen das Unternehmen ein. Denn wenn eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt wird, kann ein Bußgeld von bis zu 50.000 Euro erlassen werden.
Das Unternehmen teilte daraufhin mit, die Auskunft längst erteilt zu haben und schickte einen Screenshot der Übersichtsansicht eines E-

Mailprogramms, auf dem man die angebliche Antwortmail hätte erkennen können. Der Ordner „gesendete Objekte“ wurde angeblich gelöscht. Daher konnte der Inhalt der Auskunft an den Bürger nicht mehr hergestellt werden.
Im Laufe des Bußgeldverfahrens legte das Unternehmen nun doch noch den Inhalt der angeblich erteilten Auskunft vor. Das Bußgeldverfahren wurde vom Amtsgericht Erfurt daraufhin eingestellt.

Auch wenn ein Unternehmen seine Produkte über ein Online-Verkaufsportal anbietet, ist es zur Auskunftserteilung gegenüber dem Bürger verpflichtet.

2.40 Auskunft – sonst ...

Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Beschwerden darüber, dass Unternehmen Auskunftsersuchen gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) nicht beantworten. Ein Beschwerdeführer wollte in einem solchen Auskunftsersuchen von einem Unternehmen wissen, welche Daten über ihn bei dem Unternehmen gespeichert waren und wo sie herkamen, an wen seine personenbezogenen Daten weitergegeben wurden und den Zweck der Speicherung seiner Daten bei dem Unternehmen. Hintergrund des Auskunftsersuchens gemäß § 34 Abs. 1 BDSG war ein unerwünschter Werbeanruf. Das Auskunftsrecht ist für die Betroffenen ein fundamentales Datenschutzrecht. Dieses Recht ermöglicht ihnen die Prüfung, ob die verantwortliche Stelle, hier das Unternehmen, rechtmäßig Daten über sie verarbeitet. Das Bundesverfassungsgericht hat im Volkszählungsurteil aus Art. 2 Abs. 1 i: V. m. Art. 1 Abs. 1 Grundgesetz die Befugnis des Einzelnen abgeleitet, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmten (BVerfGE 65, 1, 41 f). Das Auskunftsrecht ist regelmäßig Voraussetzung für die Ausübung und damit selbst Bestandteil des Rechts auf informationelle Selbstbestimmung.
Da die Auskunft nicht erteilt worden war, wurde gegen das Unternehmen ein Bußgeld nach § 43 Abs. 1 Nr. 8 a BDSG in Höhe von 150,00 Euro verhängt und vollstreckt. Ferner wird gegen das Unternehmen eine Anordnung zur Auskunftserteilung erlassen.

Auskünfte auf Anfragen nach § 34 Abs. 1 BDSG dürfen nur verweigert werden, wenn das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt. Unterbliebene Auskunftserteilungen können mit einer Geldbuße von bis zu 50.000 Euro geahndet werden, § 43 Abs. 3 BDSG.

2.41 Datenklau – Mitnahme von Kundendaten bei Versicherungen

Nicht selten kommt es vor, dass ein Versicherungsmakler sich von der von ihm vertretenen Versicherung löst und künftig für ein anderes Versicherungsbüro Tätigkeiten aufnimmt. Ebenso steht es bei Versicherungsmaklern, die innerhalb der Branche wechseln.
Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner aufsichtsbehördlichen Tätigkeit von folgendem Sachverhalt Kenntnis. Die Beschwerdeführerin – ein Vermittlungsbüro – kündigte mittels einer fristlosen Kündigung einem in ihrem Betrieb tätigen selbstständigen Versicherungsvertreter. Der Versicherungsvertreter wechselte zu einem anderen Unternehmen und nahm von seinem alten Vertragspartner eine Vielzahl von Datensätzen in ausgedruckter sowie in digitaler Form mit. So unter anderem alle Kunden- und Vertragsdaten des alten Vertragspartners.
Nach bisherigem Erkenntnisstand nutzte der selbstständige Versicherungsmakler diese Daten, um Kunden werblich anzusprechen und abzuwerben. Datenschutzrechtlich betrachtet handelte es sich bei der Mitnahme der Kundendaten um eine Datenerhebung und -verarbeitung, § 3 Abs. 3 und 4 Bundesdatenschutzgesetz (BDSG). Dieser Umgang mit personenbezogenen Daten ist gemäß § 4 Abs. 1 BDSG nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Rechtsvorschrift für die Mitnahme der Kundendaten durch den Versicherungsvermittler findet sich weder im Bundesdatenschutzgesetz noch in einer anderen Rechtsvorschrift. Daher verblieb vorliegend nur noch die Möglichkeit, dass die Kunden des Versicherungsvermittlers in die Übermittlung der Datensätze zwischen dem alten Vermittlungsbüro und der Erhebung in dem neuen Vermittlungsbüro eingewilligt hatten. Nach Aufforderung des TLfDI ließ der Versicherungsvermittler dem TLfDI eine

Maklervereinbarung sowie eine Liste aller Kunden, die eine solche Einwilligung unterschrieben hatten und somit vom Versicherungsvermittler weiter betreut werden wollten, zukommen. Das Verwaltungsverfahren ist vorliegend noch nicht abgeschlossen. Die vorliegenden Einwilligungen der Kunden werden seitens des TLfDI noch ausgewertet.
Da hier auch die Verwirklichung eines Ordnungswidrigkeitentatbestandes im Raum steht und dieser darüber hinaus mit Bereicherungsabsicht erfüllt worden sein könnte, hat der TLfDI von seinem Recht, einen Strafantrag zu stellen, Gebrauch gemacht und die Staatsanwaltschaft über den Sachverhalt informiert.

Strafbares Handeln im Sinne des BDSG liegt vor, wenn zu einer Ordnungswidrigkeit gemäß § 43 Abs. 2 BDSG noch weitere Merkmale (§ 44 BDSG) hinzukommen, nämlich die dort genannten Merkmale des Handelns gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht. In diesem Fall kann der Täter mit einer Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden. Es handelt sich aber um ein Antragsdelikt, sodass eine Verfolgung durch die Strafbehörden nur nach der Stellung eines Strafantrages durch den Betroffenen selbst oder den TLfDI durchgeführt werden kann.

2.42 Insolvenzverfahren mit über die Ufer tretenden Datenflüssen

In einem Insolvenzverfahren forderte ein Insolvenzverwalter von der Insolvenzschuldnerin sämtliche Versicherungsunterlagen an. Die Insolvenzschuldnerin hatte dem Insolvenzverwalter daraufhin ALLE Versicherungsunterlagen vorgelegt, die in ihrem Besitz waren. Ohne die Versicherungsunterlagen auf Relevanz im Insolvenzverfahren zu prüfen, gab der Insolvenzverwalter diese zwei Ordner mit Versicherungsunterlagen an eine Versicherungsmaklergesellschaft weiter, damit sie den Versicherungsumfang prüfen und ggf. anpassen konnte. Unter diesen Unterlagen befand sich auch ein Versicherungsschein für das Einfamilienhaus, in dem die Insolvenzschuldnerin lebte. Allerdings war dieser auf den Namen des getrennt lebenden Ehemanns der Insolvenzschuldnerin ausgestellt. Beide Ehegatten waren Eigentümer der Immobilie. Ohne die Unterlagen auf Bezug zur Insolvenzschuldnerin zu überprüfen, hatte das Maklerunterneh-

men die Ordner aufbewahrt und ihren Auftrag zur Prüfung des Versicherungsumfangs ausgeführt.
Hier lagen gleich mehrere Verstöße gegen das Bundesdatenschutzgesetz (BDSG) vor, die getrennt voneinander geahndet wurden.
Seitens des Insolvenzverwalters lag eine unbefugte Übermittlung von personenbezogenen Daten, die nicht Bestandteil des Insolvenzverfahrens waren, an die Versicherungsmaklergesellschaft vor. Die Datenübermittlung fällt unter den Begriff der Verarbeitung von personenbezogenen Daten. Der Insolvenzverwalter war nicht befugt, die personenbezogenen Daten des Ehegatten der Insolvenzschuldnerin zu übermitteln. Nach § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Eine Einwilligung lag hier nicht vor. Die Übermittlung des Versicherungsscheins zur Prüfung des Versicherungsumfangs erfolgte auch nicht nach § 28 Abs. 1 BDSG. Sie war nicht zur Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Ehemann der Insolvenzschuldnerin erforderlich. Zwar hat die Insolvenzschuldnerin dem Insolvenzverwalter die Versicherungsunterlagen übergeben, dennoch war er zur sorgfältigen Prüfung verpflichtet, ob und welche personenbezogenen Daten zur Übermittlung an das Maklerunternehmen in Betracht kamen, um diese dann im Anschluss gezielt einzugrenzen. Der Insolvenzverwalter musste lediglich prüfen, ob ein ausreichender Versicherungsschutz der Insolvenzschuldnerin bestand. Dies wäre auch ohne Übermittlung sämtlicher Versicherungsunterlagen an die Versicherungsmaklergesellschaft möglich gewesen. Zumal die Immobilie nur zur Hälfte zur Insolvenzmasse gehörte.
Die Versicherungsmaklergesellschaft war auch nicht befugt, die personenbezogenen Daten des in Trennung lebenden Ehegatten der Insolvenzschuldnerin aufzubewahren. Eine Verarbeitung von Daten liegt nach § 3 Abs. 4 Nr. 1 BDSG unter anderem dann vor, wenn Daten gespeichert werden. Hierunter versteht man das Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Datenträger ist jedes Medium, auf dem Daten lesbar festgehalten werden können, wobei es nicht auf die Art des Lesens ankommt. Technische Instrumente sind insofern nicht notwendig. Es genügt jedes Material, das beschriftet oder in sonstiger Weise Informationen aufnehmen kann, insbesondere auch Papier (vergleiche Dammann in Simitis BDSG Kommentar,

8. Auflage, § 3, Rn. 118). Hier lag weder eine Einwilligung des Ehegatten vor, noch beruhte die Datenverarbeitung auf einer gesetzlichen Grundlage, § 4 Abs. 1 BDSG. Jedenfalls überwog das schutzwürdige Interesse des Ehegatten der Insolvenzschuldnerin an dem Ausschluss der Aufbewahrung durch die Maklergesellschaft, § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Auch wenn der Insolvenzverwalter dieses beauftragte, den bestehenden Versicherungsschutz der Insolvenzschuldnerin zu prüfen, um die Masse im Schadenfall zu erhalten, war die Maklergesellschaft zur sorgfältigen Prüfung verpflichtet, ob und welche personenbezogenen Daten zur Aufbewahrung in Betracht kamen, um diese dann im Anschluss gezielt einzugrenzen. Da die Ehefrau Insolvenzschuldnerin war, war kein Grund erkennbar, die Daten des Ehemannes aufzubewahren. Darüber hinaus war der Ehemann der Insolvenzschuldnerin nach § 33 Abs. 1 BDSG von der Speicherung, der Art der Daten, der Zweckbestimmung der Verarbeitung und der Identität der Versicherungsmaklergesellschaft zu benachrichtigen, da erstmals personenbezogene Daten für eigene Zwecke zunächst ohne Kenntnis des Betroffenen gespeichert wurden. Gegebenenfalls wäre die Weitergabe der Versicherungsunterlagen möglich gewesen, wenn zwischen Insolvenzverwalter und Versicherungsmaklergesellschaft ein Vertrag über die Auftragsdatenverarbeitung nach § 11 BDSG bestanden hätte. Ein solcher Vertrag lag jedoch nicht vor.

Auch wenn mit der Eröffnung des Insolvenzverfahrens die materielle und verfahrensrechtliche Verwaltungs- und Verfügungsbefugnis über das dem Insolvenzbeschlag unterliegende Vermögen auf den Insolvenzverwalter übergeht, muss dieser prüfen, welche personenbezogenen Daten für die Durchführung des Insolvenzverfahrens überhaupt erforderlich sind. Beim Umgang mit diesen Daten hat er sich an die allgemeinen und je nach abzuwickelndem Unternehmen an die spezifischen datenschutzrechtlichen Vorschriften zu halten.

2.43 Auskunft an den TLfDI: unverzüglich – sonst Bußgeldverfahren

In einem Fall einer Videoüberwachungsanlage hatte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an den Kamerabetreiber gewandt und um Stellungnahme zu dem vorgeworfenen Sachverhalt gebeten. Der TLfDI ist im-

mer an einer Sachverhaltsaufklärung und Problemlösung interessiert. Nicht bei allen Beschwerden kann den Wünschen des Beschwerdeführers oder Kamerabetreibers entsprochen werden. Oftmals ist aber eine Videoüberwachung gar nicht zu beanstanden, weil diese bereits den Vorgaben des Bundesdatenschutzgesetzes (BDSG) entspricht. Anstatt die Auskunftsersuchen des TLfDI nach § 38 Abs. 3 BDSG zu beantworten, stellte der Kamerabetreiber aber auf Durchzug und verwehrte dem TLfDI die Antworten. Nach § 38 Abs. 3 BDSG haben die der Kontrolle unterliegenden Stellen – auch natürliche Personen – der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Bußgeldverfahrens aussetzen würde. Darauf wird der Auskunftspflichtige vom TLfDI immer hingewiesen. Auf die Fragen des TLfDI hatte der Kamerabetreiber nicht vollständig und damit, soweit die Antwort unterblieben ist, nicht rechtzeitig geantwortet, obwohl er zu seiner Antwortpflicht in den Schreiben des TLfDI ausdrücklich belehrt wurde. Der Kamerabetreiber hatte grundsätzlich unverzüglich, vollständig und wahrheitsgemäß seiner Auskunftspflicht nachzukommen. „Unverzüglich“ bedeutet ohne schuldhaftes Zögern. In Anbetracht des Umfangs der gestellten Fragen wäre spätestens nach vier Wochen eine Auskunft zu erteilen gewesen. Abgesehen davon kann die vom TLfDI gesetzte Frist nur im Ausnahmefall und nach Absprache überschritten werden (Petri in Simitis, Kommentar BDSG, 8. Auflage, § 38, Rn. 55). Auf ein evtl. bestehendes Zeugnisverweigerungsrecht hatte sich der Kamerabetreiber nicht berufen.

Gegen den Kamerabetreiber wurde ein Ordnungswidrigkeitenverfahren nach § 43 Abs. 1 Nr. 10 BDSG durchgeführt. Danach handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 38 Abs. 1 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. Eine Auskunftserteilung unterblieb jedoch bis zum Ende des Berichtszeitraums. Parallel zum Ordnungswidrigkeitenverfahren kann der TLfDI eine Anordnung, die auf die Auskunftserteilung des Kamerabetreibers abzielt, gemäß § 38 Abs. 5 BDSG, auch unter Festsetzung eines Zwangsgeldes, erlassen.

Auskunftspflichtige haben der Aufsichtsbehörde nach § 38 Abs. 3 BDSG auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann sich dabei auf sein Auskunftsverweigerungsrecht berufen. „Unverzüglich“ bedeutet ohne schuldhaftes Zögern. In Abhängigkeit der vom TLfDI gestellten Fragen ist in der Regel nach vier Wochen eine Auskunft zu erteilen. Abgesehen davon kann die vom TLfDI gesetzte Frist nur im Ausnahmefall und nach Absprache mit ihm überschritten werden.

2.44 Offenlegung des bürgerlichen Namens – am Briefkasten manchmal ein Problem!

Frau Bauer (Name im Tätigkeitsbericht selbstverständlich geändert), Mieterin in einem Mehrfamilienhaus, beschwerte sich darüber, dass ihr bürgerlicher Name Frau Müller durch Aushänge im Hausflur des Mehrfamilienhauses offengelegt wurde. So habe Frau Bauer mit dem Vermieter vor deren Einzug in das Mehrfamilienhaus vereinbart, dass ihr Name Frau Müller im Außenverhältnis verheimlicht werde. Dazu zählten sämtliche Klingelschilder und Briefkastennamen sowie die eventuellen Namen auf Nebenkostenabrechnungen. Stattdessen wurde die Mieterin im Außenverhältnis mit ihrem Pseudonym Frau Bauer angesprochen. Nun wurde die Hausverwaltung an ein anderes Unternehmen vergeben. Eine Mitarbeiterin der neuen Hausverwaltung erkundigte sich bei der Mieterin, warum der Name Frau Müller geheim zu halten sei. Sie erklärte den Sachverhalt ausführlich und fügte hinzu, dass ihr bei Offenbarung ihres Namens Frau Müller drohe, Opfer eines Gewaltverbrechens zu werden. Diese Mitarbeiterin der neuen Hausverwaltung hatte dennoch den Namen Frau Müller gegenüber anderen Mietern und Dritten offen gelegt, indem Sie Frau Bauer / Frau Müller auf einem Putzplan benutzte. Dieser wurde im Hausflur des Mehrfamilienhauses veröffentlicht. Seitdem wurde die Post der Hausverwaltung auch nicht mehr an Frau Bauer, sondern an Frau Müller adressiert. Zudem wurden die Briefe, bei denen die Hausverwaltung Absender war, nicht ganz in den Briefkasten hinein gesteckt. Diese Briefe wurden durch die Hausverwaltung selbst in die Briefkästen der Mieter verteilt und waren bei dieser Mieterin nur soweit eingesteckt, dass die Adresse mit dem Namen Frau Müller zu sehen war. Für alle sonstigen Zustellungen gab Frau

Müller ihre Postfachadresse an. Bis dahin war sie nur unter ihrem Pseudonym Frau Bauer unter der Postanschrift zu erreichen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sah hier eine unbefugte Übermittlung nicht öffentlich zugänglicher personenbezogener Daten der Mieterin. Denn eine Verarbeitung personenbezogener Daten ist grundsätzlich unzulässig, es sei denn, das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift erlaubt oder ordnet dies an oder der Betroffene hat darin eingewilligt, § 4 Abs. 1 BDSG. Unter Verarbeiten fällt nach § 3 Abs. 4 Nr. 3 BDSG auch die Übermittlung personenbezogener Daten. Eine Einwilligung der Mieterin lag hier offensichtlich nicht vor. Die Wohnungsverwaltung konnte sich in diesem Fall auch nicht auf eine Rechtsgrundlage innerhalb oder außerhalb des BDSG stützen. Die Übermittlung des Namens der Mieterin war nach § 28 Abs. 1 Nr. 1 BDSG nicht für die Erfüllung eigener Geschäftszwecke und auch nicht nach § 28 Abs. 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen der Wohnungsverwaltung erforderlich. Außerdem standen erhebliche schutzwürdige Interessen der Mieterin der Übermittlung ihres Namens Frau Müller an die Hausbewohner und Dritte (Besucher) entgegen. Sie befürchtete, Opfer eines Gewaltverbrechens zu werden. Ein Ordnungswidrigkeitenverfahren gegen die Wohnungsverwaltung wurde daraufhin eingeleitet.

Der TLfDI kann neben dem Verwaltungsverfahren nach § 38 BDSG auch gleichzeitig Ordnungswidrigkeitenverfahren nach § 43 Abs. 1 und 2 BDSG einleiten. Daher kann es neben einer festgesetzten Geldbuße auch zur Anordnung mit Androhung eines Zwangsgeldes kommen, wenn den Aufforderungen des TLfDI nicht nachgekommen wird.

Data and privacy security. Information protection. File folder a – © Maksym Yemelyanov / Fotolia.com

3 Aktenarchivierung

3.1 Orientierungshilfe Aktenarchivierung – wie geht es weiter?

Bereits in seinem 1. Tätigkeitsbericht im nicht-öffentlichen Bereich informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter Nummer 3.1 über die Gründung des Runden Tisches „Orientierungshilfe Aktenaufbewahrung (OH A)“. Ziel war, dass der Runde Tisch eine Orientierungshilfe (OH) entwickeln wird, die zum einen Archivierungsdienstleister in die Lage versetzen sollte, datenschutzrechtlich korrekt zu arbeiten, und zum anderen Unternehmen, die diese Dienstleister beauftragen wollen, dazu befähigen sollte, die Archivierungsdienstleister einer qualifizierten Bewertung unterziehen zu können. Eine solche OH erscheint aus Sicht des TLfDI bedeutsam, da seine Erfahrungen in der Vergangenheit gezeigt haben, dass bisweilen sowohl Auftraggeber als auch Auftragnehmer nicht mit der notwendigen Sorgfalt an das Thema Aktenarchivierung und die damit zusammenhängende

Auftragsdatenverarbeitung herangehen. Der Runde Tisch war im Nachgang zu dem in Thüringen aufgedeckten insolventen Aktenlager in Immelborn gegründet worden. Ihm gehörten neben dem TLfDI Vertreter sowie Datenschutzbeauftragte von Aktenarchivierungsunternehmen an. In mehreren Sitzungen wurde eine OH entwickelt, die neben allgemeinen Aussagen zu Aufbewahrungsfristen und zur Auftragsdatenverarbeitung auch spezielle Hinweise für die Archivierung der Akten von Berufsgeheimnisträgern enthält. Ebenfalls Teil der OH sind Checklisten, die dem Unternehmer bzw. dessen betrieblichen Datenschutzbeauftragten (bDSB) eine Hilfestellung bei der Beantwortung der Frage bieten, ob personenbezogene Daten extern archiviert werden sollen. Sofern diese Entscheidung positiv ausfallen würde, finden sich Angaben zu den jeweils notwendigen technischen und organisatorischen Maßnahmen. Der TLfDI hat die vom Runden Tisch entworfene OH dem Düsseldorfer Kreis vorgestellt. Hierbei handelt es sich um einen Zusammenschluss der Aufsichtsbehörden im nicht-öffentlichen Bereich. Die Erarbeitung der OH wurde dort grundsätzlich gebilligt und auch inhaltlich im Wesentlichen für gut befunden. Allerdings gab es an der einen oder anderen Stelle noch Änderungswünsche, denen der TLfDI nachkommen wird. Sobald die OH überarbeitet wurde, wird sie dem Düsseldorfer Kreis erneut zur Entscheidung vorgelegt werden.

Das Thema Aktenarchivierung bewegte den TLfDI auch im 2. Berichtszeitraum im nicht-öffentlichen Bereich. Gemeinsam mit Vertretern von Aktenarchivierungsunternehmen hat er eine Orientierungshilfe Aktenarchivierung erarbeitet, die nach der Billigung durch den Düsseldorfer Kreis veröffentlicht werden soll.

3.2 Tatort Mülltonne – datenschutzgerechte Entsorgung?

Im Altpapier finden sich oft sensible Daten. Besonders brisant wird dies dann, wenn Berufsgruppen betroffen sind, die unter eine besondere Geheimhaltungspflicht fallen, wie z. B. Ärzte oder Rechtsanwälte.
Einem aufmerksamen und besorgten Bürger fiel eben solch ein Fall auf. Er bemerkte nur mit Vorhängeschlössern gesicherte Tonnen, die mehrere Tage auf der Straße standen. Die eingeschaltete Polizei stellte fest, dass es sich bei den Tonnen um Behältnisse zur Entsorgung von datenschutzrechtlich relevanten Unterlagen handelte. We-

nigstens eine der beiden Tonnen wies solche Mängel auf, dass ein Zugriff für jedermann auf die Dokumente in den Behältern möglich war. Im Rahmen der dann durchgeführten Ermittlungen wurde festgestellt, dass es sich um Unterlagen handelte, die einem besonderen Berufsgeheimnis unterfielen. Die Unterlagen waren 10 Jahre alt oder älter und waren daher tatsächlich zu vernichten. Die ermittelte verantwortliche Stelle gab sich auf Anschreiben des TLfDI zunächst uneinsichtig. Man habe alles richtig gemacht, man könne nichts dafür, wenn das beauftragte Unternehmen die Unterlagen nicht rechtzeitig abhole. Man habe extra ein Fachunternehmen für die Entsorgung der Akten beauftragt.
Der TLfDI klärte die verantwortliche Stelle darüber auf, dass sie im Sinne des § 1 Abs. 2 Ziff. 3 i. V. m. § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) verantwortliche nicht-öffentliche Stelle sei. Dies gelte auch dann, wenn eine Datenverarbeitung, hier eine Löschung durch ein Drittunternehmen, im Auftrag durchgeführt werde, § 3 Abs. 7 BDSG. Als verantwortliche nicht-öffentliche Stelle hat das Unternehmen technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Nach Anlage zu § 9 Satz 1 BDSG dürfen personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Indem die Unterlagen auf eine Art und Weise auf der Straße gelagert wurden, die einen Zugriff von Dritten nicht ausgeschlossen hat, musste also im Ergebnis festgestellt werden, dass die getroffenen technisch-organisatorischen Maßnahmen nicht ausreichend waren.
Dem TLfDI wurde zwischenzeitlich mitgeteilt, dass man den Vernichtungsprozess inzwischen auf andere Weise organisiert hätte. Die Unterlagen würden mithilfe eines büroeigenen Schredders vernichtet. Auf Nachfrage konnte der TLfDI sicherstellen, dass der Schredder die technischen Voraussetzungen für personenbezogene Daten, die einem Berufsgeheimnis unterfallen, erfüllt. Die Materialteilchenfläche muss in solchen Fällen kleiner/gleich 30 qmm sein. Dies entspricht der Sicherheitsstufe P-5 der DIN 66399-2 bzw. der Stufe 4 der (älteren) DIN 32757-1.
Damit ist das Verfahren abgeschlossen.

Nach dem BDSG dürfen personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen,

kopiert, verändert oder entfernt werden. Die verantwortlichen nicht-öffentlichen Stellen haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Das Abstellen von „Datensicherheitsbehältern“ auf der Straße bzw. im Hinterhof eines Unternehmens stellt gerade keine solchen getroffenen technisch-organisatorischen Maßnahmen dar, wenn Dritte unbefugt von den personenbezogenen Daten Kenntnis erlangen können. Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen, müssen nach dem Schreddern eine Materialteilchenfläche kleiner/gleich 30 qmm aufweisen. Dies entspricht der Sicherheitsstufe P-5 der DIN 66399-2 bzw. der Stufe 4 der (älteren) DIN 32757-1.

3.3 Ad Acta zu den Akten ... oder doch nicht?

Bereits im 1. Tätigkeitsbericht über den nicht-öffentlichen Bereich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde über das herrenlose Aktenlager im Thüringer Örtchen Immelborn / Wartburgkreis berichtet. Die im Sommer 2013 vorgefundene Situation hat den TLfDI auch in diesem Berichtszeitraum beschäftigt.
Der größte Teil des Jahres 2014 wurde darauf verwandt, den Aktenbestand, soweit möglich, zu sichten und den jeweils einlagernden Insolvenzverwaltern bzw. Unternehmen zuzuordnen. Diese Tätigkeit des TLfDI fand im Rahmen einer gegenüber Ad Acta angedrohten und letztlich durchgeführten Ersatzvornahme statt. Sie gliederte sich in zwei wesentliche Schritte. Zum einen mussten die vorhandenen Akten gesichtet und den jeweiligen verantwortlichen Stellen zugeordnet, zum anderen dann an diese zurückgeführt werden. Jedenfalls das Sichten der Akten war für das Erdgeschoss und das Mittelgeschoss unter schwierigen Bedingungen noch möglich, da hier ein großer Teil der Akten zum überwiegenden Teil in zugänglichen Regalen eingeordnet war, lose auf dem Boden herumlag oder in Kartons vor sich hin gammelte. Im Obergeschoss sah dies anders aus. Hier waren die Akten in Kartons auf Paletten oder in so genannten Stahlgittercontainern teilweise meterhoch gestapelt und teilweise zusammengestürzt. Ohne technisches Gerät war hier wenig bis nichts zu erreichen. Zwar konnten die meisten Kartons durch den TLfDI noch auf die jeweilige verantwortliche Stelle hin geprüft werden, jedoch spätestens bei den schweren Gitterpaletten war damit Schluss.

Um diese sowohl zeitlich, als auch vom Arbeitsvolumen her umfassende Aufgabe einerseits möglichst zügig zu erledigen, andererseits Hilfe bei den vom TLfDI nicht zu bewerkstelligenden technischen Problemen zu erhalten, bat dieser die Thüringer Polizei um Amtshilfe. Hierüber berichtete der TLfDI bereits in seinem letzten Tätigkeitsbericht. Diese wurde mit der Begründung abgelehnt, dass bei einer Unterstützung des TLfDI durch die Polizei diese ihren sonstigen Aufgaben nicht mehr nachkommen könne. Gefordert hatte der TLfDI im Übrigen lediglich zehn Personen für einen Zeitraum von zehn Tagen.

Der von der CDU beantragte und inzwischen eingesetzte Untersuchungsausschuss des Thüringer Landtages hat inzwischen jedoch herausfinden können, dass die Absage der Polizei auf Veranlassung des Staatssekretärs des Thüringer Innenministeriums (TIM) vorgenommen wurde. Tatsächlich wollte und konnte die Polizei dem TLfDI helfen, wurde aber von der politischen Spitze des Innenministeriums daran gehindert.

Das TIM versuchte, das Problem „auszusitzen“ bzw. „den Kopf in den Sand zu stecken“ und so zu verfahren, als habe es mit dem Aktendepot in Immelborn rein gar nichts zu tun. Der TLfDI akzeptierte die niedrigschwelligen Ausführungen des TIM jedoch nicht und erhob am 4. Juli 2014 Klage beim Verwaltungsgericht Weimar wegen Nichtgewährung von Amtshilfe: Doch wie kam es zu diesem ungewöhnlichen und in Deutschland bisher einmaligen Vorgehen, dass ein Landesdatenschutzbeauftragter ein Innenministerium auf Gewährung von Amtshilfe verklagte? Rückblende:

Ende August 2013 – dem TLfDI war das Aktendepot gerade zwei Monate zuvor bekannt geworden – fanden zwischen dem TLfDI und der Thüringer Landespolizeidirektion (LPD) erste Gespräche statt über eine Gewährung von Amtshilfe durch die Thüringer Polizei. Der TLfDI legte daher den Vertretern der LPD die Situation im Aktendepot von Immelborn dar und bat um personelle Unterstützung bei der Aktenbergung und -räumung durch die Thüringer Polizei, konkret durch Beamte der Bereitschaftspolizei. Mit Schreiben vom 10. September 2013 stellte der TLfDI noch einmal förmlich ein Amtshilfeersuchen bei der LPD. Eine solche Amtshilfe wollte der Präsident der LPD, dem die Bereitschaftspolizei unterstellt ist, dem TLfDI auch zunächst gewähren. Umso erstaunter war deshalb nicht nur der TLfDI, als das TIM im September 2013 den Mitgliedern des Innenausschusses des Landtages mitteilte, dass die Bereitschaftspoli-

zei keine Hilfe bei der Herstellung datenschutzkonformer Zustände im Aktendepot von Immelborn leisten könne.
Der TLfDI reagierte „zweigleisig“ auf diese abwegige Nachricht: Zum einen informierte er die Thüringer Ministerpräsidentin, den Thüringer Finanzminister und die Präsidentin des Thüringer Landtags über die Lage im Aktendepot von Immelborn und richtete an die genannten Behörden/Institutionen die Frage, ob sie dem TLfDI andere Möglichkeiten einer Amtshilfe eröffnen könnten. Die Antworten auf diese Frage des TLfDI fielen durchweg negativ aus. Zum anderen stellte der TLfDI am 21. November 2013 beim TIM einen Antrag gemäß § 5 Abs. 5 Satz 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) auf Entscheidung über die Verpflichtung der LPD zur Gewährung von Amtshilfe im Fall der Herstellung datenschutzrechtskonformer Zustände im Aktendepot von Immelborn und begründete diesen. Daneben betrieb er das eigentliche Verfahren, ordnungsgemäße Zustände in Immelborn zu erreichen, selbst weiter.
Das TIM zeigte sich jedoch weiter unkooperativ und stellte das Vorliegen der Voraussetzungen für einen Anspruch auf Amtshilfe des TLfDI in Frage. Bei zehn Mann für zehn Tage sei die Sicherheit des Freistaates nicht mehr gewährleistet. In dem Zeitraum von Dezember 2013 bis einschließlich April 2014 legte der TLfDI noch einmal in mehreren Schreiben dem TIM dar, dass die Voraussetzungen für einen Amtshilfeanspruch nach § 5 Abs. 1 Nr. 2, 1. und 2. Variante ThürVwVfG im Fall des Aktendepots von Immelborn gegeben waren.
Am damaligen TIM prallten alle Argumente des TLfDI ab und es teilte mit Schreiben vom 6. Februar und zuletzt 24. April 2014 mit, dass es keine Amtshilfe gestatte. Das TIM begründete seine Entscheidung unter anderem damit, dass das Amtshilfegesuch des TLfDI rechtsmissbräuchlich sei.
Gegen diese ablehnende Entscheidung des TIM zu seinem Amtshilfegesuch sah der TLfDI nach eingehender juristischer Prüfung gute Chancen, auf dem Rechtsweg seine Interessen durchzusetzen und mithilfe der Bereitschaftspolizei datenschutzrechtskonforme Zustände im Aktendepot von Immelborn wiederherzustellen. Der TLfDI reichte daher am 4. Juli 2014 Klage beim Verwaltungsgericht Weimar ein und beantragte, ihm die begehrte Amtshilfe in Form der Bergung, Sichtung und Sortierung der noch im Aktendepot in Immelborn lagernden, nicht erfassten Akten durch mindestens zehn Polizeibeamte der Bereitschaftspolizei sowie durch Bereitstellung

der zur Aktenbergung notwendigen technischen Hilfsmittel der Polizei im Zeitraum für mindestens zehn Arbeitstage zu gewähren.
Über diese Klage des TLfDI hatte das Verwaltungsgericht Weimar in der Sache jedoch nicht mehr zu entscheiden. Ursächlich dafür war folgende Entwicklung: Dem TLfDI war es im Herbst 2014 gelungen, einen Rechtsanwalt als Nachtragsliquidator für jene Firma zu gewinnen, die zuletzt das Aktendepot in Immelborn betrieb. Dieser Rechtsanwalt wurde sodann auf Antrag des TLfDI Ende Januar 2015 vom Amtsgericht Jena als Nachtragsliquidator bestellt. Nur unter der Regie eines Nachtragsliquidators konnten im Zeitraum vom 4. Februar zum 26. März 2015 unter Verwertung der noch vorhandenen Gegenstände die im Aktendepot von Immelborn verbliebenen Akten einer datenschutzgerechten Verarbeitung zugeführt, d. h. entweder vernichtet, rückgeführt oder unter Beachtung der Vorschriften des Bundesdatenschutzgesetzes anderweitig eingelagert werden. Dabei unterstützte der TLfDI im Rahmen seiner aufsichtsbehördlichen Beratungs- und Prüfungsaufgabe den Nachtragsliquidator bei der Auflösung des Aktendepots.
Ein Untersuchungsausschuss des Thüringer Landtags hat gemäß Art. 64 der Verfassung des Freistaats Thüringen in Verbindung mit § 1 Abs. 1 Untersuchungsausschussgesetz die Aufgabe, Sachverhalte, deren Aufklärung im öffentlichen Interesse liegen, zu untersuchen und dem Landtag darüber Bericht zu erstatten. Der TLfDI hat bei der Erledigung seiner ihm zukommenden Aufgabe, datenschutzkonforme Zustände im Aktendepot von Immelborn herbeizuführen, gute Arbeit geleistet. Der TLfDI war und ist daher gern bereit, dem Untersuchungsausschuss 6/2 des Thüringer Landtags alle erforderlichen Informationen zur Erfüllung seines Untersuchungsauftrages zur Verfügung zu stellen. Dabei wird sich dann auch zeigen, dass die Thüringer Polizei Amtshilfe leisten wollte, dieses aber von der damaligen Hausspitze des Innenministeriums verhindert wurde. Im nächsten Tätigkeitsbericht wird dieser bundesweit einmalige und tiefenscharfe Einblick in die kuriosen Funktionsmechanismen des damaligen Innenministeriums ausführlich dargestellt werden. Der Vorsitzenden des Untersuchungsausschusses Frau MdL Henfling sei bereits an dieser Stelle für ihre faire und nachfassende Verhandlungsführung gedankt.

Die Aufbewahrung von Akten stellt Unternehmen immer wieder vor praktische Probleme. Der TLfDI wird sich dafür einsetzen, dass die

unter seiner Federführung entstandene Orientierungshilfe zu diesem Thema veröffentlicht wird (siehe dazu Nummer 3.1).

3.4 Löschen, Sperren, Archivieren!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Beschwerde eines Bürgers, der bei einem Dienstleister für Personalmanagement um die Löschung seiner personenbezogenen Daten gebeten hatte. Eine eingeforderte Bestätigung der umfänglichen Löschung seiner Daten hatte er nicht erhalten. Der Bürger war Teilnehmer eines Coaching-Projekts für Einzelpersonen zur Wiedereingliederung gewesen. Auftraggeber war das Jobcenter, nach § 45 Sozialgesetzbuch (SGB) III. Der Personaldienstleister konnte dem Wunsch auf umfängliche Löschung der Daten nur bedingt Rechnung tragen, da er nach den Regelungen des Handelsgesetzbuches (§ 257 Abs. 1, 4 HGB) und der Abgabeordnung (§ 147 Abs. 2 i. V. m. Abs. 1 Nr. 1, 4 und 4a AO, § 14b Abs. 1 UStG) verpflichtet war, die Teilnehmerunterlagen zehn Jahre für Prüfungs- und Nachweiszwecke aufzubewahren. Außerdem müssen dem Jobcenter, der Prüfgruppe der Bundesagentur für Arbeit und dem Rechnungsprüfungsamt auf Verlangen und zum Nachweis der Aktivitäten des Arbeitssuchenden die Teilnehmerunterlagen vorgelegt werden können (vergleiche auch § 61 SGB II, Auskunftspflichten bei Leistungen zur Eingliederung in Arbeit). Aus diesem Grund werden die Unterlagen der Teilnehmer nach der Verweildauer im Projekt für sechs Monate in einem Ordner „ausgeschiedene Teilnehmer“ elektronisch aufbewahrt, um bei Rückfragen aussagefähig zu sein, anschließend werden die Daten auf dem Server im „Archiv“ gespeichert. Die Daten werden mit dieser Verfahrensweise nach § 35 Abs. 3 Bundesdatenschutzgesetz (BDSG) in Verbindung mit § 3 Abs. IV Nr. 4 BDSG gesperrt. Auf das Archiv haben nur der Datenschutzbeauftragte und der Administrator Zugriff. Nach zehn Jahren werden die Daten der Teilnehmer gelöscht. Gegen diese Praxis war aus datenschutzrechtlicher Sicht nichts einzuwenden.

Ein Anspruch nach § 35 Abs. 2 Bundesdatenschutzgesetz (BDSG) auf Löschung der gespeicherten Daten über eine Person kann aufgrund gesetzlicher Aufbewahrungsfristen nicht immer sofort durchgesetzt werden. Stehen der Löschung nämlich Aufbewahrungsfristen

entgegen, sind die Daten nur zu sperren und erst nach deren Ablauf zu löschen, § 35 Abs. 3 Nr. 1 BDSG.

3.5 Löschfristen versus Aufbewahrungsfristen

Die wenigsten Unternehmen, wie Banken oder Kreditinstitute, können alle Dienstleistungen selbst erbringen. Hierzu bedient man sich anderer Unternehmen, die sich auf den entsprechenden Bereich spezialisiert haben. So auch im nachfolgenden Fall. Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines solchen privaten Thüringer Dienstleistungsunternehmens. Hauptaufgabe des genannten Unternehmens sind Immobiliendienstleistungen für Banken und Kreditinstitute und in diesem Zusammenhang die Erfassung von Objektdaten, wie Fotos und Besichtigungsberichte von Immobilien. Nach Aufforderung durch die Auftraggeber soll das Dienstleistungsunternehmen diese Daten binnen einer Frist von acht Wochen nach Auslieferung endgültig löschen. Für das Unternehmen stellte sich daher die Frage, ob hier nicht insoweit eine Kollision der Löschfristen nach dem Bundesdatenschutzgesetz (BDSG) zu den gesetzlichen Aufbewahrungspflichten für Unternehmen bestehe.
Damit das BDSG überhaupt auf die gegenständlichen Daten Anwendung findet, muss es sich dabei um personenbezogene Daten handeln. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Dazu genügt es, wenn die Person nicht namentlich benannt wird, aber möglicherweise auch nur mit Zusatzwissen bestimmbar ist. Soweit das Unternehmen Adressdaten und Namen erhebt, ist der Anwendungsbereich des BDSG eröffnet. Ob es sich im dargestellten Sachverhalt bei den erfassten Objektdaten um personenbezogene Daten handelte, konnte der TLfDI anhand der bisherigen Darstellungen nicht feststellen.
Soweit personenbezogene Daten betroffen sind, sind diese nach § 35 Abs. 3 Nr. 3 BDSG zu löschen, wenn der Zweck der Speicherung entfällt. Ob und wann dann dementsprechend zu löschen ist, richtet sich nach dem individuellen Zweck und der daran anknüpfenden Erforderlichkeit im Sinne des § 28 BDSG. Nach § 28 Abs. 1 BDSG ist das Speichern personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es

für die Begründung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses zum Betroffenen erforderlich ist. Nach § 28 Abs. 1 Nr. 2 und Nr. 3 BDSG ist das Speichern personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Nr. 2) oder wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der verantwortlichen Stelle offensichtlich überwiegt (Nr. 3). Nach Auslieferung der Daten durch das Dienstleistungsunternehmen an seinen jeweiligen Auftraggeber war der Zweck der Speicherung von möglicherweise betroffenen personenbezogenen Daten entfallen. Stehen darüber hinaus dem Löschen Aufbewahrungsfristen entgegen, sind die Daten bis zum Ablauf dieser Frist zu sperren und dann zu löschen, § 35 Abs. 3 Nr. 1 BDSG. Aufbewahrungsfristen können sich aus einer Vielzahl von Rechtsgrundlagen ergeben.
Unterstellt, dass es sich bei dem Dienstleistungsunternehmen um einen Kaufmann gehandelt hat, wäre § 257 Abs. 4 Handelsgesetzbuch (HGB) einschlägig gewesen. Danach beträgt die Aufbewahrungsfrist sechs Jahre. Mit der Beratungsleistung war das Verfahren für den TLfDI abgeschlossen.

Personenbezogene Daten sind zu löschen, wenn der Zweck der Speicherung entfällt. Stehen diesem Löschen Aufbewahrungsfristen entgegen, sind die Daten zu sperren und erst nach Ablauf der Aufbewahrungsfrist endgültig zu löschen.

Security Camera, CCTV on location, airport – © alice_photo / Fotolia.com

4 Videoüberwachung

4.1 Endlich eine Orientierungshilfe (OH) zur Videoüberwachung

Bereits im letzten Berichtszeitraum war bei allen Aufsichtsbehörden im nicht-öffentlichen Bereich zu beobachten, dass die Videoüberwachung einen immer größeren Stellenwert einnimmt. Dies lag sicherlich auch daran, dass Kameras und Videoüberwachungssysteme zu immer günstigeren Preisen angeboten wurden. Größere Unternehmen haben Filialen in mehreren Bundesländern. Besonders sie waren daran interessiert, dass die datenschutzrechtliche Beurteilung der Videoüberwachung von den Aufsichtsbehörden im Bundesgebiet einheitlich vorgenommen wird. Die Datenschutzkonferenz rief daher eine Ad-hoc-AG Videoüberwachung als Unterarbeitsgruppe des Düsseldorfer Kreises ins Leben. Diese Arbeitsgruppe sollte sich mit speziellen Fragen der Videoüberwachung befassen und dafür sorgen, dass unbestimmte Rechtsbegriffe im Bundesgebiet von Aufsichtsbehörden möglichst einheitlich ausgefüllt werden. Schnell war man

sich einig, dass es einer Orientierungshilfe bedarf, um das komplexe Feld der Videoüberwachung datenschutzrechtlich möglichst bundeseinheitlich bewerten zu können. Es gibt im Wesentlichen drei Bestimmungen, nach denen sich die datenschutzrechtliche Beurteilung einer Videoüberwachung richtet:
Dies sind § 6b Bundesdatenschutzgesetz (BDSG) für die Videoüberwachung in öffentlich zugänglichen Bereichen, § 28 BDSG für die Videoüberwachung in öffentlich nicht zugänglichen Bereichen und § 32 BDSG für den Fall, dass Mitarbeiter überwacht werden. Alle drei Bestimmungen enthalten einige unbestimmte Rechtsbegriffe, die es auszufüllen galt. In mehreren Sitzungen wurde die OH „Videoüberwachung durch nicht-öffentliche Stellen“ erarbeitet und schließlich vom Düsseldorfer Kreis mit Stand vom 19. Februar 2014 beschlossen. Die OH ist auf der Homepage des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) unter https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh-v__-durch-nicht-__ffentliche-stellen.pdf veröffentlicht. Der TLfDI hat an der Erarbeitung der OH mitgearbeitet und legt sie bei den datenschutzrechtlichen Prüfungen von Videoüberwachungen in Thüringen zugrunde. Dort sind die Anforderungen an eine datenschutzgerechte Videoüberwachung niedergelegt. Weiterhin gibt es einige Ausführungen zu Spezialfällen, wie beispielsweise zu Webcams, zur Videoüberwachung in Gaststätten, Videoüberwachung von Beschäftigten und zur Videoüberwachung durch Vermieter. Am Ende findet sich eine Checkliste für den Betreiber einer Videoüberwachung öffentlich zugänglicher Räume. Anhand einer Frageliste kann geprüft werden, ob eine datenschutzgerechte Videoüberwachung möglich ist. Falls noch Zweifel bestehen, kann immer noch die Aufsichtsbehörde gefragt werden, da das Ausfüllen der Checkliste keine Garantie für die Rechtmäßigkeit der Überwachungsmaßnahme bietet.

Im Berichtszeitraum stellte sich schnell heraus, dass es weitere Sonderprobleme der Videoüberwachung gibt. Die Ad-hoc-AG wurde daher verstetigt und tagt nunmehr regelmäßig. Sie hat für zwei weitere Bereiche potentieller Videoüberwachung Regelungen getroffen. Zum einen wurde die OH „Videoüberwachung in öffentlichen Verkehrsmitteln“ erarbeitet und vom Düsseldorfer Kreis mit Stand vom

16. September 2015 beschlossen (siehe Anlage 3), zum anderen wurde ein Zusatz zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ zur Videoüberwachung in Schwimmbädern erarbeitet. Dieser Zusatz ist unter https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/01_zusatz_zur_oh_v__.pdf auf der Homepage des TLfDI veröffentlicht. In dem Zusatz werden ergänzend zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ spezielle Probleme, die in Schwimmbädern auftauchen, datenschutzrechtlich beurteilt. Bereits in seinem 9. Tätigkeitsbericht zum Datenschutz im öffentlichen Bereich hatte der TLfDI unter Nr. 5.5 über die Schwierigkeiten bei datenschutzrechtlichen Kontrollen in Frei- und Hallenbädern berichtet. Nunmehr liegen auch hier bundeseinheitliche Anforderungen vor und der TLfDI kann bei seinen Prüfungen nun die mit den anderen Aufsichtsbehörden abgestimmten Anforderungen anwenden.

Die AG Videoüberwachung hat unter Mitarbeit des TLfDI die OH „Videoüberwachung durch nicht-öffentliche Stellen“ erarbeitet, mit der nunmehr bundeseinheitliche Anforderungen für die datenschutzrechtliche Zulässigkeit einer Videoüberwachung vorliegen. Ergänzt wird diese OH durch einen Zusatz für die Videoüberwachung in Schwimmbädern und mit der OH „Videoüberwachung in öffentlichen Verkehrsmitteln“. Alle potentiellen Betreiber einer Videoüberwachungsanlage sind gut beraten, sich zunächst mit den dort niedergelegten Anforderungen vertraut zu machen.

4.2 Video im Bus – kein Muss – Videogaga 1

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine anonyme Anzeige gegen ein Busunternehmen in Thüringen ein. Der Eigentümer des Unternehmens habe kürzlich neue Fahrzeuge angeschafft und in diesen Videotechnik installiert. Dabei werde das komplette Innere des Busses einschließlich des Sitzes des Busfahrers überwacht. Außerdem werde auch noch ein Teil des Straßenbereichs vor dem Bus aufgenommen. Der TLfDI stattete dem Busunternehmen einen Besuch ab und kon-

trollierte dort die vom Unternehmen durchgeführte Videoüberwachung. Dabei stellte sich heraus, dass zur Objektsicherung des Betriebsgeländes 14 Kameras zum Einsatz kamen. Die in der anonymen Anzeige gemachten Angaben bestätigten sich vor Ort. Die modernen Busse des Unternehmens waren mit einer Videoüberwachung ausgestattet, die sowohl die Fahrgäste als auch den Busfahrer überwachte. Auch ein Teil des Straßenbereichs vor dem Bus wurde mit aufgezeichnet. Der Inhaber des Unternehmens teilte mit, dass er hinsichtlich der Überwachung in den Bussen davon ausgegangen sei, dass diese unproblematisch sei, da die Fahrzeuge mit der entsprechenden Ausstattung angeboten worden seien und die Ausrüstung der Fahrzeuge auch durch ein Förderprogramm des Freistaates Thüringen mit 75 Prozent der Anschaffungskosten gefördert worden sei.
Im Rahmen des Arbeitskreises Verkehr erfuhr der TLfDI zwischenzeitlich, dass die Videoüberwachungen in Bussen und sonstigen Unternehmen des öffentlichen Personennahverkehrs auch in anderen Ländern deutlich zugenommen hat. Auch die Aufsichtsbehörden der anderen Länder sahen das Bedürfnis, für diesen Bereich einheitliche Festlegungen zu treffen. Die Aufsichtsbehörden beschlossen daher, eine Orientierungshilfe für die Videoüberwachung im öffentlichen Personennahverkehr zu erarbeiten (siehe Anlage 9) Der TLfDI stellte das Verfahren der Prüfung der Videoüberwachung des Busunternehmens aus diesem Grund zunächst zurück, um das Ergebnis der Beratungen über die Orientierungshilfe abzuwarten. Nachdem die Orientierungshilfe vom Düsseldorfer Kreis beschlossen wurde, trat der TLfDI erneut an das Busunternehmen heran und bat dieses zunächst, die auf dem Betriebsgelände und in den Dienstbussen aktuell durchgeführte Videoüberwachung nochmals darzulegen. Es war nicht ausgeschlossen, dass sich aufgrund des Zeitablaufs zwischenzeitlich Änderungen ergeben hatten. Der TLfDI wird die durchgeführte Videoüberwachung anhand der Festlegungen der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ prüfen. Es ist davon auszugehen, dass eine lückenlose Überwachung des Busfahrers jedenfalls nicht zulässig sein wird, da nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz personenbezogene Daten eines Beschäftigten zur Aufdeckung von Strafdaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Für das Unternehmen wird außerdem schwer zu begründen sein, warum der öf-

fentliche Verkehrsraum mitüberwacht werden muss und eine nahezu lückenlose Überwachung der Busse durchgeführt wird. Das weitere Verfahren bleibt abzuwarten.

Auch im öffentlichen Personennahverkehr ist eine Videoüberwachung nicht grundsätzlich zulässig, sie muss im Rahmen geltender Datenschutzgesetze durchgeführt werden. Der TLfDI wird die in der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ festgelegten Grundsätze bei der Prüfung zugrunde legen.

4.3 Herausgabe von Daten aus Videoüberwachungsanlagen an Strafverfolgungsbehörden – Videogaga 2

Im April 2014 hatte sich ein externer Datenschutzbeauftragter an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt und um Aufklärung zum Thema „Herausgabe und Einsichtnahme von Daten aus einer Videoüberwachung oder gespeicherten Daten von Kunden, Mitarbeitern oder Ähnlichem an Strafverfolgungsbehörden“ gebeten. Dieser Datenschutzbeauftragte berät Thüringer Unternehmen bei der Umsetzung und Gestaltung des Datenschutzrechts in der Praxis.
Im Ergebnis ist die Polizei oftmals berechtigt, die Herausgabe von Aufnahmen einer Videoüberwachung zum Zwecke der Strafverfolgung zu verlangen. Die Polizeibehörden haben die Aufgabe, Straftaten zu erforschen, § 163 Abs. 1 S. 1 StPO i. V. m. § 2 Abs. 1 Polizeiaufgabengesetz (PAG), d. h., sie sind im Falle eines Anfangsverdachts verpflichtet, den Sachverhalt umfassend selbstständig zu erforschen und die Maßnahmen zu treffen, welche zur Aufklärung der Straftat erforderlich sind. Damit ist die Polizei der „verlängerte Arm der Staatsanwaltschaft“. Die Ermittlungen der Polizei und der Staatsanwaltschaft bilden eine Einheit. Zu ihren allgemeinen Ermittlungen bzw. Ermittlungsbefugnissen gehört unter anderem das Herausverlangen von Gegenständen nach § 95 Abs. 1 der Strafprozessordnung (StPO). Diese Vorschrift betrifft Beweisgegenstände nach § 94 Abs. 1, Abs. 2 StPO. Beweismittel sind alle beweglichen und unbeweglichen Gegenstände, die unmittelbar oder mittelbar für die Tat oder die Umstände ihrer Begehung Beweis erbringen. Hierzu zählen auch Videoaufnahmen, welche die Straftat dokumentiert haben. Jeder Gewahrsamsinhaber von Beweismitteln hat die Pflicht zur Vorlage und Herausgabe auf Anforderung der Ermittlungsbehör-

den. Einer Beschlagnahmeanordnung bedarf es hierfür nicht. Eine Beschlagnahme nach § 94 Abs. 2 StPO ist nur erforderlich, wenn die Videoaufnahmen nach Aufforderung der Strafverfolgungsbehörden nicht herausgegeben werden. Dabei setzt der Verhältnismäßigkeitsgrundsatz dem staatlichen Handeln wegen der besonderen Eingriffsintensität Grenzen. Die Beschlagnahme muss sich auf die Daten beschränken, die für die Verfolgung einer Straftat erforderlich sind. Der Zugriff auf alle anderen auf einem Datenträger enthaltenen Daten muss im Rahmen des Vertretbaren vermieden werden. Weiterhin muss die Beschlagnahme in angemessenem Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen und für die Ermittlungen notwendig sein. Der Tatverdacht muss eine Tatsachengrundlage haben, aus der sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt. Eine bloße Vermutung reicht nicht aus (Meyer-Goßner StPO, 58. Auflage, § 94, Rn. 18).

Voraussetzungen der Herausgabe an die Strafverfolgungsbehörden:

Soweit ein Polizist sich bei einer nicht-öffentlichen Stelle ausweist und mündlich erklärt, dass z. B. eine Anzeige wegen Körperverletzung vorliegt, die Videoüberwachung die Tat aufgenommen hat und zu Beweiszwecken verwendet werden soll, ist nach der rechtlichen Grundlage der Datenerhebung mittels der Kamera zu differenzieren. Sofern mit einer Kamera personenbezogene Daten erhoben werden, also z. B. Personen oder Kfz-Kennzeichen erkennbar sind, bedarf es nach dem so genannten Verbot mit Erlaubnisvorbehalt einer rechtlichen Grundlage für die Übermittlung an die Polizeibehörde. Zu unterscheiden ist dabei zwischen der Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen (§ 6b des Bundesdatenschutzgesetzes [BDSG]), der Videoüberwachung von Beschäftigten (§ 32 Abs. 1 BDSG) und einer sonstigen Videoüberwachung in nicht öffentlich zugänglichen Räumen (§ 28 BDSG).
Eine wesentliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welche die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Nach § 6b BDSG erhobene personenbezogene Daten können nur nach § 6b Abs. 3 Satz 2 BDSG einer Zweckänderung unterfallen. Für einen anderen Zweck dürfen sie danach nur verarbeitet (übermittelt) oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit sowie zur

Verfolgung von Straftaten erforderlich ist. Nach Auffassung des TLfDI können nicht-öffentliche Stellen auf diese Möglichkeit der Zweckänderung zurückgreifen und rechtmäßig erhobenes Videomaterial an die Ermittlungsbehörden zum Zweck der Strafverfolgung übermitteln. Eine Übermittlung personenbezogener Videoaufnahmen nach Satz 2 kann weder an private Sicherheitsdienste noch an Privatpersonen zur Erleichterung der Verfolgung ihnen gegenüber verübter Straftaten erfolgen.
Eine verantwortliche nicht-öffentliche Stelle (z. B. ein Unternehmen) kann Videodaten nach § 28 BDSG für eigene Geschäftszwecke aufzeichnen. Die für eigene Geschäftszwecke erhobenen Videodaten enthalten in der Regel Aufnahmen von nicht-öffentlich zugänglichem Raum. Diese erhobenen personenbezogenen Daten können nach § 28 Abs. 2 Nr. 2b BDSG übermittelt oder genutzt werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist und schutzwürdige Belange des Betroffenen nicht entgegenstehen. Diese Bestimmung gilt aber nur für die für eigene Geschäftszwecke erhobenen Videodaten, die eher die Ausnahme darstellen dürften. Nach § 28 Abs. 2 Nr. 2b BDSG müssen konkrete Anhaltspunkte für das Vorliegen einer Gefahr oder Straftat gegeben sein. Bei Videoaufzeichnungen ist eine besonders gewissenhafte Interessenabwägung vorzunehmen. Da sich in aller Regel auch Daten von nicht verdächtigen Personen auf den Aufnahmen befinden, muss es sich um eine Straftat von einer gewissen Schwere handeln. Allein die Verfolgung von Ordnungswidrigkeiten oder ein bloßer Gefahrenverdacht ist als Zweck nicht ausreichend (Simitis in Simitis, Kommentar BDSG, 8. Auflage, § 28, Rn. 190). Die Norm des § 28 BDSG stellt allerdings keine Erhebungsbefugnis für die Polizei oder die Staatsanwaltschaft dar, sondern dient als Übermittlungsbefugnis, wenn eine nicht-öffentliche Stelle Videoaufnahmen ohne Aufforderung durch die Staatsanwaltschaft oder die Polizei dorthin übermittelt.
Strafverfolgungsbehörden bedürfen einer eigenen Rechtsgrundlage, um Videomaterial herausverlangen zu dürfen. Solche eigenen bereichsspezifischen Eingriffsbefugnisse ergeben sich aus der StPO und den Polizeigesetzen der Länder.

Aufnahmen aus Videoüberwachungsanlagen von nicht-öffentlichen Stellen können nach § 6b Abs. 3 Satz 2 BDSG im Rahmen einer Zweckänderung an Strafverfolgungsbehörden übermittelt werden.

Danach dürfen Videoaufnahmen allerdings nicht an private Sicherheitsdienste oder an Privatpersonen übermittelt werden. Bei Videoüberwachungsanlagen, die Daten nach § 28 Abs. 1 BDSG erheben und speichern, gibt es ebenfalls eine geeignete Übermittlungsbefugnis an die Strafverfolgungsbehörden nach § 28 Abs. 2 Nr. 2b BDSG, wenn konkrete Anhaltspunkte für das Vorliegen einer Gefahr oder Straftat gegeben sind.

4.4 Diamantenfieber – Videogaga 3 – Videoüberwachung eines Juweliers

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Beschwerde eines Bürgers über eine Videoüberwachung mit zwei Kameras, die an einem Gebäude angebracht waren und möglicherweise den öffentlichen Verkehrsbereich überwachten. Der TLfDI ermittelte zunächst den Eigentümer des Gebäudes. Es stellte sich heraus, dass in dem Gebäude ein Juweliergeschäft betrieben wird. Der Inhaber des Geschäftes teilte auf Nachfrage mit, dass das Thüringer Landesverwaltungsamt die von ihm durchgeführte Videoüberwachung im Jahr 2011 geprüft und in datenschutzrechtlicher Hinsicht gebilligt hatte. Der damalige Schriftwechsel mit dem Thüringer Landesverwaltungsamt wurde dem TLfDI zur Kenntnis übermittelt. Daraus ergab sich nicht, welchen Bereich die vor dem Gebäude angebrachten Kameras tatsächlich erfassen. Wie bereits unter 15. dargelegt, haben die Datenschutzaufsichtsbehörden der Länder im Düsseldorfer Kreis die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ beschlossen (s. auch Anlage 3). In dieser Orientierungshilfe wird bundeseinheitlich darüber informiert, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Der TLfDI prüfte die am Haus angebrachte Videoüberwachung vor Ort, um zu kontrollieren, ob die Maßgaben der Orientierungshilfe eingehalten wurden. Dabei wurde festgestellt, dass die eine Kamera durch Blumen aus einem Blumenkasten so verhängt ist, dass außer den Blumen nichts auf dem Bild zu sehen ist. Die andere Kamera war so ausgerichtet, dass teilweise der ganze Bereich des Bürgersteigs aufgezeichnet wurde. Nach § 6b Bundesdatenschutzgesetz (BDSG) ist die Videoüberwachung öffentlich zugänglicher Bereiche zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Soll eine Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin ein berechtigtes Interesse zu sehen. Eigentlich ist hierfür aber eine tatsächliche Gefahrenlage zu fordern. In bestimmten Fällen ist auch eine abstrakte Gefährdungslage ausreichend, wenn es sich um eine Situation handelt, die nach der Lebenserfahrung typischerweise gefährlich ist. Dies ist z. B. in Geschäften der Fall, die, wie Juweliere, wertvolle Ware verkaufen. Daher ist es grundsätzlich zulässig, wenn ein Juwelier seine Auslage im Schaufenster durch eine Videoüberwachung schützt. Allerdings muss die Videoüberwachung auch so ausgerichtet sein, dass schutzwürdige Interessen Dritter nicht beeinträchtigt werden. Der TLfDI hat den Juwelier daher gebeten, die Kameras so auszurichten, dass nur ein schmaler, maximal ein Meter breiter Streifen vor dem Schaufenster von der Videoüberwachung erfasst ist. Auf diese Weise – so die Rechtsprechung - bleibt ein größerer Teil des Bürgersteiges frei von Aufzeichnungen. Personen, die den Bürgersteig benutzen, können der Videoaufzeichnung ausweichen.

Es ist grundsätzlich zulässig, wenn ein Juwelier seine Auslage im Schaufenster durch eine Videoüberwachung schützt, allerdings darf der überwachte Bereich sich nur auf das Notwendige beschränken und den öffentlichen Verkehrsraum nur maximal einen Meter erfassen.

4.5 Nächtliche Videoüberwachung eines Betriebsgeländes – kein Videogaga 4

Eine Gemeinde erhielt eine anonyme Anzeige über eine Videoüberwachung auf einem ehemaligen Bahnhofsgelände. Dieses Schreiben leitete die Gemeinde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter. Nach Recherchen des TLfDI konnte der Eigentümer des Grundstücks ausfindig gemacht werden, der dort Materialien lagerte, die für den von ihm durchgeführten Gewerbebetrieb benötigt wurden. Trotz intensiven Schriftwechsels mit dem Betreiber der Videoüberwachung konnte der Vorgang nicht abschließend behandelt werden, da sich die örtlichen Verhältnisse aufgrund der eingegangenen Schreiben und eingereichten Lagepläne nicht eindeutig ermitteln ließen. Bei einem

Vorortttermin wurde festgestellt, dass das Grundstück, auf dem die Videoüberwachung durchgeführt wurde, nicht öffentlich zugänglich war. Das Grundstück war vollständig eingezäunt und die Zugänge zu dem Grundstück waren verschlossen. In der Vergangenheit war es vermehrt zu Diebstählen der dort gelagerten Materialien gekommen. Seitdem die Videoüberwachung installiert worden war, kam es nicht mehr zu derartigen Vorfällen. Eine Videoaufzeichnung fand nur in den Nachtstunden von 20:00 Uhr bis 6:00 Uhr morgens statt. Die Aufnahmen wurden nach 72 Stunden wieder überschrieben. Im Aufnahmebereich der Kameras befanden sich der Eingang zu einer auf dem Grundstück befindlichen Lagerhalle sowie der Zugang zum Bahnhofsgebäude.
Da das Grundstück komplett umzäunt und verschlossen war, handelt es sich nicht um einen öffentlich zugänglichen Bereich, sodass § 6b Bundesdatenschutzgesetz (BDSG) keine Anwendung fand. Der Anwendungsbereich des BDSG war jedoch eröffnet, da das Grundstück für den Gewerbebetrieb des Betreibers genutzt wurde. Die Videoüberwachung ist mit § 28 Abs. 1 Nr. 2 BDSG vereinbar. Der Schutz des Eigentums vor Diebstahl ist ein berechtigtes Interesse der verantwortlichen Stelle. Da hier lediglich die Eingänge zu den auf dem Grundstück befindlichen Gebäuden beobachtet wurden und die Aufzeichnung nur während der Nachtzeit stattfand, besteht kein Grund zur Annahme, dass schutzwürdige Interessen potenziell von der Videoüberwachung Betroffener beeinträchtigt sind. Der Betreiber der Videoüberwachungsanlage hatte auch keine Angestellten, daher standen auch Arbeitnehmerinteressen einer Videoüberwachung nicht entgegen. Der TLfDI teilte der Gemeinde mit, dass die Videoüberwachung mit den datenschutzrechtlichen Bestimmungen vereinbar war.

Im nicht öffentlich zugänglichen Bereich richtet sich die Zulässigkeit der Videoüberwachung nach § 28 BDSG. Der Schutz des Eigentums vor Diebstahl ist ein berechtigtes Interesse im Sinne dieser Vorschrift. Allerdings dürfen schutzwürdige Interessen der von der Videoüberwachung Betroffenen im Rahmen der Abwägung nicht überwiegen. Bei einer nächtlichen Videoüberwachung eines Betriebsgeländes scheiden solche schutzwürdigen Interessen in der Regel aus.

4.6 Rundum überwachte Lebensmittel – Videogaga 5

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war mit einem Fall von Videoüberwachung in einem Lebensmittelladen befasst, der nach § 6b Bundesdatenschutzgesetz (BDSG) zu beurteilen war. Die Kommunikation war in diesem Fall besonders schwierig, weil der Inhaber des Ladens mehrfach wechselte. Zunächst erhielt der TLfDI auf seine Anfrage nur eine sehr spärliche Auskunft. Ein längerer Abstimmungsprozess mit den wechselnden Marktinhabern begann. Ursprünglich war ein Kamerasystem mit 22 Kameras in der letzten Ausbaustufe vorgesehen. Es gab keine schriftliche Festlegung dazu, wer Zugriff auf die Aufzeichnungen hat und unter welchen Voraussetzungen die Aufzeichnungen eingesehen werden können. Auch die mit einer Detektei geschlossene Vereinbarung zur Auftragsdatenverarbeitung entsprach nicht den gesetzlichen Anforderungen des § 11 BDSG. Aufgrund der Intervention des TLfDI reduzierte der Marktinhaber die Zahl der zum Einsatz kommenden Kameras auf acht. Er ließ von dem bestellten betrieblichen Datenschutzbeauftragten (bDSB) eine Vorabkontrolle für den Einsatz von Videosystemen nach § 4 d Abs. 5 BDSG durchführen. Darin wurde festgelegt, welche Personen unter welchen Voraussetzungen Zugriff auf die Videoaufzeichnungen haben und wie diese vor fremdem Zugriff geschützt werden. Bereiche, in denen sich Beschäftigte des Marktes ständig aufhalten, wie z. B. der Kassenbereich, waren vom Aufnahmebereich der Kameras ausgenommen. Ebenso war nicht der komplette Markt der Videoüberwachung ausgesetzt, sondern es gab auch überwachungsfreie Bereiche. Allerdings bezog sich die Videoüberwachung nicht nur auf Regale, in denen sich besonders wertvolle Lebensmittel, wie z. B. Spirituosen, befanden. Dies begründete der Markt damit, dass eine wirksame Verhinderung von Diebstählen nur möglich sei, wenn der Täter ständig mit der Beobachtung und Entdeckung seiner Tat rechnen müsse. Es sei nicht auszuschließen, dass Personen Waren zunächst in den Warenkorb legen und diese dann in anderen Bereichen des Marktes verschwinden lassen. Aufgrund der getroffenen technischen und organisatorischen Maßnahmen, das heißt der schriftlichen Festlegung in der Vorabkontrolle sowie der Tatsache, dass bestimmte Bereiche des Marktes von der Videoaufzeichnung ausgenommen waren, konnte der TLfDI die Angelegenheit im Berichtszeitraum als erledigt erklären.

Wichtig ist bei der der Videoüberwachung auch im Lebensmittelladen, dass keine Anhaltspunkte dafür bestehen dürfen, dass schutzwürdige Interessen der Kunden oder Beschäftigten überwiegen. Dem kann dadurch begegnet werden, dass die Videoüberwachung auf das erforderliche Maß beschränkt wird und keine festen Arbeitsplätze dauerhaft überwacht werden. Wichtig ist auch, schriftlich festzulegen, wer unter welchen Voraussetzungen die Aufzeichnungen zu welchem Zweck verwerten darf.

4.7 Mit dem Auszug war die Kamera verschwunden – Videogaga 6

Ein Mieterschutzverein wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Am Balkon eines Mehrfamilienhauses befinde sich seit geraumer Zeit eine Videokamera. Es bestand der Verdacht, dass die Kamera auf den Zugang des Gebäudes gerichtet ist, in dem sich das Büro des Mieterschutzbundes befindet und damit eventuell nachvollzogen werden sollte, ob und wann sich die Mieter des Gebäudes an selbigen wenden. Die vom TLfDI angeschriebene Immobiliengesellschaft teilte mit, dass der derzeitige Mieter der betreffenden Wohnung die Kamera installiert habe, ohne das Einverständnis des Eigentümers einzuholen. Der Mieter habe an seinem vor dem Haus abgestellten Fahrzeug mehrfach mutwillige Beschädigungen vorgefunden. Die Immobiliengesellschaft wies nach, dass sie den Mieter mehrfach aufgefordert hatte, die Kamera zu entfernen, allerdings ohne Erfolg. Der TLfDI schrieb nun den Mieter direkt an, der daraufhin lediglich mitteilte, es handele sich um eine Attrappe.
Auch wenn es sich bei der Kamera um eine Attrappe handelte, entfällt damit nicht die Pflicht zur Beantwortung der Fragen des TLfDI. Aufgrund des auch von Attrappen ausgehenden Überwachungsdrucks auf Betroffene und deren mit richtigen Kameras identischen Außenwirkung, sind diese nicht anders zu behandeln, als funktionierende Kameras. Der Mieter wurde daher erneut zur Auskunftserteilung aufgefordert. Dieses Schreiben kam als unzustellbar zurück. Nachforschungen ergaben, dass der Mieter nicht mehr in der betreffenden Wohnung wohnte. Der TLfDI ging davon aus, dass die Kamera entfernt worden war und bat den Mieterschutzverein um entsprechende Stellungnahme, falls dies nicht der Fall sein sollte. Da

keine entsprechende Rückmeldung des Mieterschutzvereins einging, konnte der Fall abgeschlossen werden.

Attrappen sind wegen des von ihnen ausgehenden Überwachungsdrucks grundsätzlich nicht anders zu behandeln als funktionierende Kameras. Es besteht auch beim Einsatz von Attrappen die Pflicht zur Beantwortung der Fragen des TLfDI.

4.8 Ferien unter Beobachtung – Videogaga 7 – Zum Einsatz von Wildkameras

Der Besitzer einer Ferienanlage beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über mehrere Wildkameras, die im umliegenden Waldgebiet installiert worden waren. Da die für den Einsatz der Kameras verantwortliche Stelle nicht ohne Weiteres ersichtlich war, wandte sich der TLfDI an das für die Gemarkung zuständige Forstamt. Das Amt wurde über die beim Einsatz von Wildkameras in Wäldern unter Nummer 4.9 beschriebene Rechtslage unterrichtet und um Mitteilung gebeten, welche Stelle für den Betrieb der Kameras verantwortlich ist. Wie sich aus der Antwort des Forstamtes ergab, waren die Wildkameras vom Inhaber eines Jagderlaubnisscheins für den Pirschbezirk installiert worden. Der Jäger gab danach an, dass ihm die Rechtslage nicht bekannt gewesen sei und er die Kameras lediglich angebracht hatte, um den Wildbestand und die Aktivitätszeiten des Wildes feststellen zu können. Ohne dass der TLfDI hier nochmals tätig werden musste, wurden die Kameras von dem Jäger entfernt. Dies wurde dem TLfDI dann auch vom Beschwerdeführer so bestätigt. Aufgrund der zu diesem Zeitpunkt recht neuen Materie hinsichtlich des Einsatzes von Wildkameras und weil der Jäger sofort rechtmäßige Zustände hergestellte, konnte der TLfDI darauf verzichten, gegen den Jäger ein Ordnungswidrigkeitenverfahren einzuleiten.

Beim Einsatz von Wildkameras müssen die datenschutzrechtlichen Bestimmungen eingehalten werden. Hierüber hat der TLfDI ausführlich sowohl den Thüringer Landesjagdverband e. V. als auch das zuständige Thüringer Ministerium für Infrastruktur und Landwirtschaft unterrichtet. Bei einem unzulässigen Einsatz von Wildkameras durch private Jäger wird der TLfDI die Einleitung von Ordnungswidrigkeitenverfahren prüfen.

4.9 Und im Wald da sind die Kameras – Videogaga 8 – Zum Einsatz von Wildkameras

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seinem 1. Tätigkeitsbericht für den nicht-öffentlichen Bereich unter 3.52 bereits auf die bestehende Problematik beim Einsatz von Wildkameras in Thüringer Waldgebieten hingewiesen. Bei weiteren Anfragen und Beschwerden von Bürgern stellte sich heraus, dass in den überwiegenden Fällen private Jäger die Fotofallen installieren. Um möglichst flächendeckend die private Jägerschaft zu erreichen, hatte sich der TLfDI daraufhin an den Landesjagdverband Thüringen e. V. gewandt, in dem viele Jäger organisiert sind. Der Verband wurde auf die bei einem geplanten Einsatz von Wildkameras zu beachtenden Rechtsvorschriften hingewiesen. Danach ist das Betreten des Waldes zunächst grundsätzlich nach Maßgabe des § 6 Thüringer Waldgesetz jedem gestattet. Es handelt sich also hier um einen öffentlich zugänglichen Raum. Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch nicht-öffentliche Stellen, worunter auch der Einsatz von Wildkameras durch private Jäger fällt, beurteilt sich daher nach § 6b Bundesdatenschutzgesetz (BDSG). Zwar haben die Jäger ein berechtigtes Interesse daran, unter Verwendung von Wildkameras den Bestand und den Wechsel des Wildes im Jagdbezirk festzustellen und die Ergebnisse für Jagd- und Hegemaßnahmen zu verwerten. Leider machen die Kameras aber nicht nur dann Bilder, wenn sich ein Wildtier dem Auslösebereich der Kamera nähert, sondern auch dann, wenn es sich um Waldspaziergänger, Pilzesucher, Waldarbeiter usw. handelt. Diese betroffenen Personen haben ein überwiegendes schützenswertes Interesse daran, sich im Wald unbeobachtet von elektronischen Einrichtungen aufzuhalten. Es muss niemand hinnehmen, sich auf einem von einer Wildkamera geschossenen Foto verewigt zu sehen, womöglich noch bei einer Handlung, die manch einer abseits der vorgegebenen Waldwege erledigt. Die Zulässigkeit des Einsatzes von Wildkameras kann in den Waldbereichen gegeben sein, die ausschließlich und erkennbar vom Jagdrevierinhaber und Jagdausübungsberechtigten betreten werden dürfen. Denkbar ist eine Zulässigkeit auch, wenn die Kameras so aufgestellt sind, dass eine Beobachtung von Personen praktisch ausgeschlossen ist, etwa in sehr

entlegenen Waldgebieten. Ist in Einzelfällen die Installation von Wildkameras erlaubt, so ist zusätzlich zu beachten, dass der Umstand der Beobachtung und die hierfür verantwortliche Stelle durch geeignete Maßnahmen erkennbar gemacht werden. Dies ist im Regelfall durch das Anbringen von deutlich sichtbaren Schildern gewährleistet. Der Landesjagdverband Thüringen e. V. wurde schließlich darauf hingewiesen, dass der in nicht datenschutzrechtlich zulässiger Weise erfolgende Einsatz von Wildkameras durch den TLfDI als Ordnungswidrigkeit mit einer Geldbuße geahndet werden kann. Der Landesjagdverband hat seine Mitglieder auf Empfehlung des TLfDI im Maiheft „Thüringer Jäger“ (5-2015) im Schwerpunktthema „Wildkamera“ über die entsprechende Rechtslage unterrichtet.

Der Wald steht grundsätzlich allen Bürgern für Erholungszwecke zur Verfügung. Diese haben ein schutzwürdiges Interesse daran, sich dort unbeobachtet von Wildkameras aufzuhalten. Der Betrieb der von der Jägerschaft eingesetzten Kameras muss Vorgaben des BDSG erfüllen, unzulässig eingesetzte Kameras sind unverzüglich zu deinstallieren. Zuwiderhandlungen werden mit einer Geldbuße geahndet.

4.10 Wo sich Wolf und Wildkatze gute Nacht sagen – Videogaga 9 – Zum Einsatz von Wildkameras

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht, dass ein Naturschutzverband in einem bestimmten Waldbereich in Thüringen Wildkameras betreibt. Dies ergab sich ebenfalls aus mehreren Zeitungsartikeln und den eigenen Angaben des Verbandes auf der vom ihm betriebenen Internetseite. Hierbei bestand die Gefahr, dass auch Privatpersonen von den Kameras erfasst und so auf unzulässige Weise in ihrem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz verletzt wurden. Handelt es sich beim Betreiber der Videokamera um eine nichtöffentliche Stelle, wie beispielsweise um einen Verein, ist das Bundesdatenschutzgesetz (BDSG) anwendbar. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des Bundesdatenschutzgesetzes oder der Betroffene hat in den Vorgang eingewilligt (so genanntes Verbot mit Erlaubnis-

vorbehalt). Es gilt hierbei das Interesse des Betreibers an der Datenerhebung mit den entgegenstehenden schutzwürdigen Interessen der Betroffenen (z. B. Spaziergänger, Sporttreibende, Pilz- und Kräutersammler) daran, sich im Wald unbeobachtet von technisch-elektronischen Einrichtungen aufzuhalten, abzuwägen. Grundsätzlich ist diese Abwägung zugunsten der betroffenen Personen vorzunehmen. Um beurteilen zu können, inwieweit die von dem Naturschutzverband betriebenen Kameras mit dem BDSG in Einklang zu bringen sind, forderte der TLfDI diesen auf, verschiedene Fragen hinsichtlich des Zwecks des Kameraeinsatzes und der dabei eingesetzten Technik, der Anzahl und der örtlichen Lage der Kameras, der erfassten Bereiche, des Personenkreises, der Zugriff auf die Bilder hat, der Speicherungsdauer usw. zu beantworten. Der Naturschutzverband versicherte dem TLfDI in seiner Stellungnahme, dass er dem Datenschutz den Vorrang vor wissenschaftlicher Erhebung von Daten über Wildtiere in den Wäldern gebe. Die Kameras seien auch nur über einen kurzen Zeitraum und lediglich als Wildtierkamerafalle in einem gut versteckten und unzugänglichen Waldgebiet, mit der Zustimmung des zuständigen Jagdpächters und der unteren Naturschutzbehörde des betroffenen Landkreises, eingesetzt worden. Personen seien durch die wenigen erstellten Wildkameraaufnahmen nicht fotografiert worden. Die Wildkameras sollen bereits nach kurzer Zeit abmontiert und nicht mehr vom Naturschutzverband in Benutzung gewesen sein. Da der Einsatz der Wildkameras bereits beendet war, teilte der TLfDI dem Verband mit, dass sich die Sache damit erledigt hatte. Ergänzend wies der TLfDI darauf hin, dass eine nicht-öffentliche Stelle die Vorgaben nach § 4 BDSG zu beachten habe. Es bedarf demnach zur zulässigen Datenerhebung einer gesetzlichen Erlaubnisnorm oder der Einwilligung der betroffenen Personen. Im Falle von betriebenen Wildkameras kommt § 6b BDSG als Rechtsgrundlage in Betracht, dessen Voraussetzungen vorliegen müssen. Auch machte der TLfDI den Verband zur Vermeidung etwaiger Ordnungswidrigkeitenverfahren nach § 43 Abs. 1 Nr. 1 BDSG darauf aufmerksam, dass es sich beim Betrieb von Wildkameras um ein automatisiertes Verarbeitungsverfahren handelt, welches nach § 4d Abs. 1 BDSG vor Inbetriebnahme dem TLfDI gemeldet werden muss, wenn keine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten stattgefunden hat. Der Inhalt dieser Meldung richtet sich nach § 4e BDSG. Die Meldepflicht entfällt nach

§ 4d Abs. 2 BDSG dann, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

Die Installation von Wildkameras ist für nicht-öffentliche Stellen nur zulässig, wenn die in § 6b BDSG genannten Voraussetzungen vorliegen und die dort genannten Maßnahmen ergriffen wurden. Ohne eine Vorabkontrolle durch einen bestellten Datenschutzbeauftragten muss ein automatisiertes Verarbeitungsverfahren vor Inbetriebnahme dem TLfDI gemeldet werden.

4.11 Wissbegieriges Vogelhäuschen – Videogaga 10 - Videoüberwachung durch den Nachbarn

Eine Beschwerde von einem besorgten Nachbarn erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Ein Grundstückseigentümer fühlte sich von seinem Nachbarn beobachtet und belästigt, weil der eine Videokamera in einem Vogelhäuschen sieben Meter weit von seiner Grundstücksgrenze aufgebaut hatte. Der Beschwerdeführer fühlte sich in seiner Privatsphäre extrem gestört, weil die Kamera den öffentlichen Bereich und sein Grundstück erfasse. Nach Überprüfung des Sachverhalts wurde festgestellt, dass nur das eigene Grundstück und ein Teil der Straße vor dem Grundstück videografiert wurde. Damit ist zwar der Beschwerdeführer nicht in dem Maße, wie angenommen, in seinem Recht auf informationelle Selbstbestimmung eingeschränkt, dennoch war die Einstellung der Kamera nicht mit dem geltenden Recht vereinbar. Der Nachbar wurde dazu aufgefordert, den Erfassungsbereich des öffentlichen Verkehrsraums auf maximal einen Meter vor der eigenen Grundstücksgrenze zu beschränken.
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von nicht-öffentlichen Stellen (Unternehmen, Privatpersonen) regelt das Bundesdatenschutzgesetz (BDSG), soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben. Der TLfDI hat hingegen keine Zuständigkeit, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13 ist diese Regelung allerdings eng auszulegen. Entscheidend ist nach diesem Urteil, ob auch Personen von der Videokamera erfasst werden können, die

in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Wie in der Pressemitteilung „Weihnachtsgeschenk für den Datenschutz!“ (siehe Anlage 19) am 11. Dezember 2014 bekannt gegeben, ist das BDSG immer einschlägig und der TLfDI damit zuständig, wenn Personen videoüberwacht werden, die mit dem Videobetreiber nicht in einer persönlichen/familiären Nähebeziehung stehen. Denn diese Art der Videoüberwachung fällt in den Anwendungsbereich der Europäischen Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes; sie ist damit nur unter den dort geregelten Voraussetzungen zulässig.

Der Aufnahmebereich der hier kontrollierten Kamera erfasste zum Teil die Straße vor dem Grundstück des Nachbarn des Beschwerdeführers. Da sich der Aufnahmebereich über das eigene Grundstück hinaus erstreckte, hatte der Nachbar keinen Einfluss darauf, wer sich in diesen Bereich hineinbewegt. Es bestand die Möglichkeit, dass Dritte in den Aufnahmebereich der Kamera gelangen können, etwa Spaziergänger, Anwohner oder Besucher, und dass diese Personen ohne rechtliche Grundlage videografiert wurden.

Nach § 4 Abs. 1 BDSG ist eine Videoüberwachung grundsätzlich wie jeder Umgang mit personenbezogenen Daten nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung durch eine gesetzliche Vorschrift erlaubt wird. Ist keine der beiden Voraussetzungen gegeben, so ist die Videoüberwachung unzulässig. Eine Einwilligung kommt der Natur der Sache nach nicht in Betracht. Es kommt also nur eine Zulässigkeit aufgrund einer Erlaubnisnorm in Betracht. Als Erlaubnisnorm kommt vorliegend nur der § 6b BDSG in Frage. Demnach ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Die hier gegenständliche Videoüberwachung sollte zu Beobachtungszwecken in Form eines verlängerten Auges als präventives Mittel dienen, um sehen zu können, wer klingelt und Kontakt mit den Bewohnern des Einfamilienhauses wünscht.

Allerdings musste die Videoüberwachung auch erforderlich sein um den vorgenannten Zweck zu erreichen. Die Kamera wurde aus Sicherheitsgründen installiert, um frühzeitig zu erkennen, ob Hausierer

den Zutritt zum eigenen Grundstück wünschen und entschieden werden kann, die Tür zu öffnen oder eben nicht. Die Erforderlichkeit einer Videoüberwachungsanlage kann zudem nur bejaht werden, wenn keine gleich wirksamen Mittel in Betracht kommen, die weniger stark in das Recht auf informationelle Selbstbestimmung Dritter eingreifen. Zu dem hier verfolgten Zweck, stellt sich keine mögliche Alternative dar, die weniger in Rechte Dritter eingreift. Zumal die Videobeobachtung in den eingeschränkten Zeiten von 8 bis 21 Uhr durchgeführt wurde. Selbst wenn eine Erforderlichkeit der Videokamera gegeben war, konnte sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Erfassungsbereich der Kamera ging über das eigene Grundstück hinaus. Auf dem von der Kamera aufgenommenen Bild war die Straße vor dem Grundstück ersichtlich. Wie oben bereits dargestellt, hatte der Betreiber der Kamera keinen Einfluss darauf, wer sich in diesen Bereich hineinbewegt. Dies stellte einen Eingriff in das Persönlichkeitsrecht der Passanten und/oder der Nachbarn bzw. der Anwohner dar. Das Amtsgericht Berlin-Mitte hat am 18. Dezember 2013 (Aktenzeichen 16 C 427/02) entschieden, dass eine Videoüberwachungsanlage im öffentlichen Verkehrsraum einen ein Meter breiten Streifen entlang der Straßenseite sowie einen ein Meter breiten Streifen links und rechts der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen darf. Darüber hinaus überwiegen insoweit die schutzwürdigen Interessen Dritter am Ausschluss einer Videobeobachtung die Interessen des Betreibers, zu sehen, wer bei ihm klingelt.
Ferner fehlte ein eindeutiges Hinweisschild, das den Umstand der Videoüberwachung sowie die verantwortliche Stelle erkennen lässt, § 6b Abs. 2 BDSG. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Bei Benennung der verantwortlichen Stelle auf dem Hinweisschild ist entscheidend, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist der Betreiber der Kamera als verantwortliche Stelle mit seinen Kontaktdaten explizit auf dem Hinweisschild zu nennen. Bei der Anbringung des Hinweisschildes ist darauf zu achten, dass dieses gut sichtbar ist und in Augenhöhe befestigt wird.

Im Ergebnis ist die Kamera erst mit den datenschutzrechtlichen Bestimmungen des Bundesdatenschutzgesetzes vereinbar, wenn der Blickwinkel der Kamera derart verändert wird, dass der Erfassungsbereich höchstens einen Meter über das Grundstück des Betreibers hinausgeht. Dem Betreiber wurde die Möglichkeit zur Stellungnahme gegeben und den Erfassungsbereich der Kamera zu ändern und ein Hinweisschild, welches den oben genannten Forderungen des § 6b Abs. 2 BDSG genügt, anzubringen. Andernfalls wurde ihm die Anordnung dessen gemäß § 38 Abs. 5 BDSG angedroht.
Die Beschwerde konnte noch nicht abschließend bearbeitet werden. Daher bleibt abzuwarten, ob der Grundstückseigentümer den Hinweisen des TLfDI folgt oder ein Verwaltungsakt erlassen werden muss. Jedenfalls hat der Grundstückseigentümer zwischenzeitlich ein Hinweisschild angebracht.

Videokameras sind heutzutage leider allgegenwärtig. Aber nicht nur im unternehmerischen Bereich sind sie auf dem Vormarsch, sondern auch in privaten Haushalten halten sie immer mehr Einzug. Dabei darf aber nicht vergessen werden, dass auch für die meisten „privaten“ Anwendungen von Videokameras die Regeln das Datenschutzrechts zu beachten sind. Werden diese nicht eingehalten, drohen Verwaltungs- und Ordnungsverfahren. Noch dazu setzt man sich der Gefahr aus, dass man von seinen Mitbürgern zivilrechtlich in die Haftung genommen wird, vergleiche §§ 823, 1004 Bürgerliches Gesetzbuch.

4.12 Auf allen Kameras blind – Videogaga 11 – die Auflösung der Kamera ist entscheidend

Das Ordnungsamt einer Gemeinde trat an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran, weil auf dem Gebiet dieser Gemeinde eine Videoüberwachung an einem Verkaufsgeschäft festgestellt worden war. Es war nicht klar, was die Kameras aufnehmen. Der Inhaber des Geschäfts wurde vom TLfDI angeschrieben. Er äußerte sich auf die gestellten Fragen nur knapp und teilte mit, dass angebrachten Kameras zur Abschreckung gegen Vandalismus dienten und eine Aufzeichnung der Daten nie stattgefunden habe. Da der Sachverhalt in weiterem Schriftwechsel nicht aufgeklärt werden konnte, führte der TLfDI eine Vorortkontrolle durch. Dabei wurde festgestellt, dass durch die

vorhandenen Kameras lediglich eine Beobachtung stattfindet. Der Inhaber des Geschäfts konnte nachweisen, dass es einen Einbruchsversuch in seinem Geschäft gegeben hatte. Ferner gab er an, dass es in der Vergangenheit Schmierereien an den Wänden und Müllablagerungen auf seinem Grundstück gegeben habe. Die Auflösung der Kameras war, da es sich um sehr alte Modelle handelte, so schlecht, dass ein Personenbezug im Hinblick auf die Personen, die sich jeweils im Aufnahmebereich der Kamera befanden nicht möglich war. Dem Inhaber des Geschäfts wurde aufgegeben, an dem Gebäude jeweils Hinweisschilder so in Augenhöhe anzubringen, dass Betroffene vor dem Betreten des überwachten Bereiches auf den Umstand der Beobachtung hingewiesen werden. Die Gemeindeverwaltung wurde über den Sachverhalt informiert.

Eine Videobeobachtung stellt einen wesentlich geringeren Eingriff in das Recht auf informationelle Selbstbestimmung dar, als dies bei Videoaufzeichnungen der Fall ist.

4.13 Die Drohne droht – Videogaga 12

Ein Fotograf wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Mitteilung, welche rechtlichen Grundlagen er bei einem gewerblichen Einsatz einer Kameradrohne beachten müsse, mit der Luftbilder von Sehenswürdigkeiten in Thüringer Städten angefertigt werden sollen. Nach Auffassung des TLfDI bestehen aus datenschutzrechtlicher Sicht hiergegen keine Bedenken, soweit ausschließlich öffentliche Plätze, öffentliche Gebäude, Denkmale usw. mit der Drohne fotografiert werden und dabei keine personenbezogenen Daten erhoben werden. Der Fotograf wurde gleichfalls darauf hingewiesen, dass bei der Erstellung von Aufnahmen, die private Grundstücke zeigen oder wenn sich auf den Bildern einzelne Personen identifizieren lassen, eine Erhebung und Verarbeitung personenbezogener Daten erfolgt. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Sowohl nach den Bestimmungen über die Beobachtung öffentlich zugänglicher Räume nach § 6b BDSG als auch nach den Regelungen des § 28 Abs. 1 Nr. 2 BDSG über die Wahrung berechtigter Interessen

der verantwortlichen Stelle, überwiegt im Regelfall das schutzwürdige Interesses der Betroffenen das berechtigte Interesse des verantwortlichen Betreibers der Fotodrohne. Besteht gar die Absicht, private Grundstücke, Parks, Gebäude oder Personen mit der Drohne zu filmen oder zu fotografieren, muss daher zuvor eine Einwilligung bei den Betroffenen eingeholt werden. Bei Aufnahmen von Personen sind insbesondere die Normen des Kunsturhebergesetzes (KunstUrhG) zu beachten, die als bereichsspezifische Regelungen entsprechend § 1 Abs. 3 Satz BDSG den Bestimmungen des BDSG vorgehen und somit etwa auch dann zur Anwendung kommen, wenn das Filmen oder Fotografieren von personenbezogenen Daten ausschließlich für private oder familiäre Zwecke erfolgt. Danach dürfen Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Voraussetzungen und Formvorschriften für eine Einwilligung bestimmen sich hierbei nach § 4a BDSG, da das KunstUrhG keine näheren Formvorschriften zur Einwilligung enthält. Zur Nutzung von Kameradrohnen durch Private wird auch auf den Beschluss der Aufsichtsbehörden im nicht-öffentlichen Bereich (siehe Anlage 8) sowie auf die Presserklärung des TLfDI vom 30. Januar 2015 (siehe Anlage 21) hingewiesen.

Eine rechtskonforme Drohnennutzung durch Private ist in Deutschland nur unter äußerst engen Voraussetzungen zulässig. Grundsätzlich darf niemand gegen seinen Willen mit einer Drohne gefilmt oder fotografiert werden.

4.14 Konzertbesuch ohne Beobachtung – Videogaga 13

In Veranstaltungsgebäuden treffen sich manchmal auch zwielichtige Gäste. Dies kann dann für den Veranstalter mit Problemen behaftet sein. Entweder kommt es auf der Veranstaltung zu unschönen Vorfällen oder das Gebäude wird im Nachgang der Veranstaltung Gegenstand von Schmierereien durch Graffiti oder Ähnlichem. In einem Fall versuchte sich der Inhaber des Gebäudes dadurch zu helfen, dass er eine Videoüberwachungsanlage installierte. Die zuständige Verwaltungsgemeinschaft informierte die Polizei, die die Angelegenheit wiederum dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) meldete. Der Anzeige waren Lagepläne und Fotos der zum Einsatz kommenden vier Kame-

ras beigefügt. Der Eigentümer des Grundstücks, auf dem sich das Gebäude befand, wurde vom TLfDI angeschrieben. Er teilte mit, dass er die Anlage noch nicht in Betrieb genommen habe. Im weiteren Verfahren wurde mit dem Inhaber reger Schriftverkehr zur Zulässigkeit der Videoüberwachung nach § 6b Bundesdatenschutzgesetz (BDSG) geführt. Da der Inhaber die Videoüberwachungsanlage demnächst in Betrieb nehmen wollte, musste er dem TLfDI alle zur datenschutzrechtlichen Beurteilung erforderlichen Informationen zukommen lassen. Insbesondere wurde der Inhaber darauf hingewiesen, dass eine Vorabkontrolle nach § 4d Abs. 5 BDSG erforderlich sei, da die vorgesehene Videoaufzeichnung einen intensiven Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen bedeute. Auch bedurfte es der Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB). Dieser Forderung des TLfDI kam der Veranstalter nach. Der von ihm bestellte betriebliche Datenschutzbeauftrage reichte die geforderte Vorabkontrolle der Videoüberwachung ein. Aber auch damit waren nicht alle gesetzlichen Anforderungen erfüllt. Der Inhaber musste zunächst Nachweise erbringen, dass es tatsächlich an seinem Gebäude in der Vergangenheit zu Schäden gekommen war. Er musste genau darlegen, welche Kameras in welchem Umfang auf öffentlich zugängliche Bereiche gerichtet waren. Weiterhin musste ein Screenshot des Aufzeichnungsbildes jeder Kamera zugesandt werden. Diesen Anforderungen kam der Grundstückseigentümer nach und der Fall konnte abgeschlossen werden.

Auch wenn eine Kamera erforderlich ist, um ein berechtigtes Interesse des Betreibers zu wahren, muss immer noch eine Abwägung mit den Interessen der von der Videoaufzeichnung Betroffenen durchgeführt werden.

4.15 Dashboard-Kameras – Verkehrsüberwachung zum Eigenbedarf – Videogaga 14

Sie verbreiten sich in Autos – die schwarzen Kästen auf dem Armaturenbrett mit dem kleinen Objektiv an der Windschutzscheibe. Dashcams sind kompakte Videoaufzeichnungsgeräte, deren Anschaffungskosten relativ niedrig sind und die auf einem Ringspeicher permanent das Verkehrsgeschehen der Straße aufzeichnen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informations-

freiheit (TLfDI) ist als datenschutzrechtliche Aufsichtsbehörde auch für den nicht-öffentlichen Bereich zuständig. Das Bundesdatenschutzgesetz (BDSG) ist nur dann nicht anwendbar, wenn die Datenverarbeitung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Es ist indes nicht plausibel, warum diese Form der Videoüberwachung lediglich zu rein familiären oder privaten Zwecken erfolgen soll. Vielmehr versprechen sich die Käufer der Dashcams hiermit, bei der Beweissicherung im Falle eines Unfalls oder einer Nötigung durch andere Verkehrsteilnehmer einen Vorteil zu erlangen. Weiterhin findet die Beobachtung und Aufzeichnung im öffentlich zugänglichen Verkehrsraum statt, wobei im Regelfall fremde Personen betroffen sind, die in keiner familiären oder privaten Beziehung zu dem Betreiber der Videokamera stehen. Mit dieser Problematik haben sich auch die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) intensiv beschäftigt und hierzu in dem Beschluss „Unzulässigkeit von Videoüberwachung aus Fahrzeugen (so genannte Dashcams)“ Hinweise bekannt gemacht (siehe Anlage 4 dieses Tätigkeitsberichts). Danach ist der Einsatz von Dashcams an den Regelungen des § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG zu messen. Im Ergebnis überwiegt im Regelfall das schutzwürdige Interesse der Verkehrsteilnehmer daran, nicht „ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden.“ Das berechtigte Interesse des Betreibers einer Dashcam in seinem Fahrzeug, ggf. als Beweismittel Videoaufnahmen vorlegen zu können, kann diesen Eingriff in das Recht auf informationelle Selbstbestimmung der anderen Verkehrsteilnehmer nicht rechtfertigen. Diese Auffassung vertritt auch das Verwaltungsgericht Ansbach in seinem Urteil vom 12. August 2014 (Az.: 4 K 13.01634). Es stellt fest, dass die Verwendung einer Dashcam einen schwerwiegenden Verstoß gegen die datenschutzrechtlichen Vorschriften darstellt. Dies gelte, obwohl der Zweck, Beweismittel bei einem Verkehrsunfall oder bei einem anderen verkehrsrechtlichen Sachverhalt vorlegen zu können, wohl als berechtigtes Interesse anzuerkennen ist. Denn die schutzwürdigen Interessen der anderen Verkehrsteilnehmer mit ihrem Recht auf informationelle Selbstbestimmung überwiegen die Interessen des Kameranutzers auf Beschaffung von Beweismitteln.

Unabhängig von der datenschutzrechtlichen Beurteilung liegt die Beantwortung der Frage, ob ein solches Video überhaupt als Beweismittel zugelassen werden kann, im Ermessen des zuständigen

Richters. Die Rechtsprechung hierzu ist uneinheitlich. So hat das Landgericht Heilbronn in seinem Urteil vom 17. Februar 2015 (Az.: I 3 S 19/14) festgestellt, dass Aufzeichnungen einer in einem Pkw installierten Dashcam im Zivilprozess nicht als Beweismittel zum Hergang eines Unfalls verwertet werden können. Das Amtsgericht Nienburg hat in einem Strafverfahren mit Urteil vom 20. Januar 2015 (Az.: 4 Ds 155/14) den Videomitschnitt einer Dashcam als Beweissicherung zugelassen. Entscheidend war hier die Tatsache, dass der Zeuge die Dashcam erst eingeschaltet hatte, nachdem der Angeklagte ihn bedrängte.

Aus datenschutzrechtlicher Sicht ist die Videoüberwachung aus Fahrzeugen durch Privatpersonen im öffentlichen Verkehrsraum grundsätzlich verboten. Der TLfDI würde in Fällen, in denen Autofahrer mit einer im Fahrzeug installierten Dashcam permanent Videoaufzeichnungen aus dem öffentlichen Verkehrsraum heraus erstellen, die Einleitung eines Ordnungswidrigkeitenverfahrens prüfen.

4.16 Drei Augen sehen mehr als zwei – Videogaga 15 – zu Dashcams

Immer wieder fragen nicht-öffentliche Stellen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob Autokameras (sog. Dashcams) in Fahrzeugen zulässig sind. So auch im vorliegenden Fall. Hier beabsichtigte ein Wach- und Sicherheitsdienst Autokameras in die Dienstfahrzeuge einzubauen. Nach Aussage des Wach- und Sicherheitsdienstes sei es nicht die Absicht, öffentliche Straßen oder Ähnliches zu überwachen, vielmehr soll mit den Autokameras eine lückenlose Nachweisführung der Tätigkeit der Mitarbeiter, das Nachvollziehen der Fahrstrecke und eventuell auch die objektive Darstellung einer vorgefundenen Situation erfolgen. Vor allem sei es in der Vergangenheit immer wieder zu Beschädigungen an den Dienstfahrzeugen gekommen, daher wären die Dashcams für eine exakte Beweis- und Nachweisführung dieser Vorkommnisse notwendig.
Der TLfDI musste in der Vergangenheit feststellen, dass die Installation solcher Kameras in Fahrzeugen, die durch die Front- und/oder Heckscheibe während der Fahrt permanent personenbezogene bzw. personenbeziehbare Daten der übrigen Verkehrsteilnehmerinnen und -teilnehmer im laufenden Verkehrsgeschehen erheben und speichern,

um mit diesen Bilddaten bei etwaigen Schadensfällen Haftungsfragen und Verantwortlichkeiten klären zu können, zugenommen hat. Eine gesetzliche Grundlage für einen solchen Einsatz von Videokameras im öffentlichen Verkehrsraum gibt es allerdings nicht. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben hierzu im Februar 2014 den Beschluss "Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)" gefasst (zu finden unter https://www.tlfdi.de/imperia/md/content/daten-

https://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/enschliessungendk/beschluss_dashcams.pdf, siehe auch Anlage 4). Aus der Überlegung heraus, dass hier bei dem Betreiben von Autokameras ein rein privates Handeln vorliegen könnte, wird oft diskutiert, ob ein Einsatz mangels Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) zulässig sein kann. Gestützt wird diese Annahme darauf, dass die Erhebung, Verwendung oder Nutzung personenbezogener Daten nach § 1 Abs. 2 Nr. 3 BDSG nicht dem Anwendungsbereich des BDSG unterfällt, wenn dies ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.

In einer am 11. Dezember 2014 ergangenen Entscheidung hat der Europäische Gerichtshof (EuGH, Urteil vom 11. Dezember 2014, C212/13), klargestellt, dass jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre des Betreiber gerichtet ist, unter den Anwendungsbereich der Europäischen Datenschutzrichtlinie und damit in den des BDSG fällt (Anlage 19). Somit war für den TLfDI klar, dass die systematische Videoüberwachung zu dem Zweck, die Aufnahmen ggf. weiterzugeben, um sich eine vorteilhaftere Rechtsposition zu verschaffen, nicht für ausschließlich persönliche Zwecke erfolgte. Daher sind Fälle, in denen die Aufnahme zu dem Zweck erfolgt, die Videodaten im Streitfall zur Dokumentation des Unfallhergangs zu verwenden, nach dem BDSG zu beurteilen.

Nach § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Voraussetzungen für eine zulässige Videoüberwachung mittels Dashcams sind

nicht erfüllt. Denn grundsätzlich hat jeder Mensch das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Letzteres würde im Falle der Nutzung von Dashcams jedoch geschehen: Mit diesen Kameras würde permanent eine Vielzahl von Personen, die sich im öffentlichen Verkehrsraum aufhalten, die keinen Anlass zu dieser Maßnahme gegeben haben und in keinem Zusammenhang zu einem etwaigen Unfallgeschehen stehen, erfasst und dabei sämtlich unter einen Generalverdacht gestellt. Zudem würden diese Personen von der Überwachung regelmäßig weder Kenntnis erlangen noch könnten sie sich dieser entziehen, da nicht in geeigneter Weise nach § 6b Abs. 2 BDSG auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden kann. Das Interesse einer Fahrzeugführerin oder eines Fahrzeugführers, vorsorglich Beweise für den individuell eher seltenen Fall des Eintritts eines Verkehrsunfalls zu sichern, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der übrigen Verkehrsteilnehmenden nicht rechtfertigen. Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht private Personen oder Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.
Diese Rechtsauffassung wurde dem Wach- und Sicherheitsdienst mitgeteilt, der sich daraufhin nicht mehr gemeldet hat. Was nicht bedeutet, dass sich der TLfDI dort nicht mehr melden wird.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallherganges angegeben wird, ist der Einsatz, auch wenn die Kameras von Privatpersonen eingesetzt werden, an den Regelungen des Bundesdatenschutzgesetzes zu messen und daher grundsätzlich rechtswidrig.

4.17 Beulen im Blech – Videogaga 16 – Kameraattrappen auf dem Parkplatz

Am 15. Dezember 2014 wandte sich ein Handelsunternehmen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Das Unternehmen richtete eine Anzeige wegen Verstoßes gegen den Datenschutz gegen einen ortsansässigen Lebensmittelbetrieb. Einmal mehr ging es um Videokameras, mit denen öffentliche Straßen, Wege, Parkanlagen und private Grundstücke überwacht werden. So jedenfalls der Vorwurf in der Anzeige. Wie üblich wurde der Lebensmittelbetrieb als verantwortliche Stelle im Sinne des § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) vom TLfDI angeschrieben und um Auskunft auf Basis von § 38 Abs. 3 BDSG gebeten. Der Lebensmittelhersteller reagierte fristgerecht und legte dar, dass es sich um Kameraattrappen handele, die installiert wurden, um eine abschreckende Wirkung zu erreichen. Deshalb sei auch zusätzlich ein Schild angebracht worden mit dem Hinweis, dass der öffentlich zugängliche Parkplatz videoüberwacht werde.
Der TLfDI verwies darauf, dass zum Recht auf informationelle Selbstbestimmung gehöre, dass dem Einzelnen bekannt ist, wer, was, wann und bei welcher Gelegenheit über ihn weiß. Genau dies sei bei einer Kameraattrappe nicht gewährleistet, da unbeteiligte Dritte den Eindruck bekommen können, aufgenommen zu werden. Der Betroffene werde deshalb versuchen, sich anders als normalerweise zu verhalten, um nicht aufzufallen. Somit gehe von einer Attrappe die gleiche Wirkung aus, wie von einer funktionsfähigen Kamera. Der TLfDI klärte auf, dass für den Schutz vor Einbrüchen, Diebstählen oder Vandalismus durch Videoüberwachungsanlagen zwar ein berechtigtes Interesse nach § 6b Abs. 1 Nr. 3 BDSG beim Betreiber zu sehen sei. Dies setze jedoch voraus, dass gegenüber dem TLfDI eine tatsächliche Gefahrenlage nachgewiesen werde, z. B. durch Belege über besondere Vorkommnisse der Vergangenheit. Das Lebensmittelunternehmen führte daraufhin drei Vorfälle von Sachbeschädigungen an Fahrzeugen von Mitarbeitern an, konnte jedoch keine Belege für die Beulen im Blech vorlegen. Im Zuge der Landesgartenschau wurden die Kameraattrappen und das Schild vom Eigentümer abgebaut. Der Parkplatz diente hierfür als Besucherparklatz. Die Firma verzichtete später auf die erneute Installation, sodass für den TLfDI kein weiterer Handlungsbedarf bestand.

Parkplatzüberwachungen durch Videoanlagen sind weit verbreitet. Oft sollen Kameraattrappen helfen, Diebstahl und Vandalismusschäden zu vermeiden. Rechtlich sind sie wie funktionsfähige Kameras zu bewerten. Ein möglicherweise berechtigtes Interesse des Betreibers muss durch den Nachweis von Rechtsverstößen belegt sein.

4.18 Baufortschritt per Webcam – Videogaga 17

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichen als Aufsichtsbehörde gemäß § 38 Bundesdatenschutzgesetz (BDSG) auch immer wieder allgemein gehaltene Anfragen zu Videokameras in Unternehmen.
Informationsbedarf bestand für Mitarbeiter einer Firma, deren Neubau des Firmengebäudes von einer Videokamera überwacht wurde, damit Interessierte den Fortgang des Baugeschehens im Internet verfolgen konnten.
Durch Einsicht in die im Internet verfügbaren Bilder des Neubaus war nicht festzustellen, dass ein offensichtlicher Datenschutzverstoß vorlag. Personen auf der Baustelle waren nicht eindeutig zu erkennen. Vielmehr wurde der Baufortschritt im Zeitraffer dargestellt.
Nach Hinweis auf die Orientierungshilfen des Düsseldorfer Kreises „Videoüberwachung durch nicht-öffentliche Stellen“ (siehe auch Anlage 3), abrufbar auf der Homepage des TLfDI über Themen/Orientierungshilfen sowie des Landesbeauftragten für den Datenschutz und Informationsfreiheit Nordrhein-Westfalen „Sehen und gesehen werden“, abrufbar auf dessen Homepage, hatte sich das Beratungsinteresse offenbar erledigt.

Die genannten Orientierungshilfen beantworten allgemeine Fragen zur Zulässigkeit von Videoüberwachungen. Es lohnt sich, sich dort zuerst zu informieren. Bleiben Fragen offen, steht hierfür der TLfDI zur Verfügung.

4.19 Was geht auf der Baustelle – Videogaga 18

Ein Mieter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er sich von einer Baustellenkamera belästigt fühlte. Auf dem Nachbargrundstück seiner Wohnanlage befände sich eine größere Baustelle, auf der zwei viergeschossige Häuser errichtet würden. Dort sei eine Kamera auf-

gestellt worden. Es gab am Bauzaun lediglich ein Schild mit der Information, dass die Baustelle videoüberwacht, nicht jedoch, wer verantwortliche Stelle für die Videoüberwachung sei. Der Betroffene habe versucht in Erfahrung zu bringen, wer für die Aufstellung der Kameras verantwortlich sei, konnte dies aber nicht ermitteln. Daher bat er den TLfDI um Hilfe.

Der TLfDI wandte sich mit einem Auskunftsersuchen nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) an den Bauherren, um nähere Einzelheiten zur durchgeführten Videoüberwachung zu erfahren. Die Baugesellschaft teilte daraufhin mit, es sei eine Fotokamera im Einsatz, die alle zwei Minuten ein Bild der Baustelle fertige. Die Aufnahmen erfolgten zum Schutz vor Einbrüchen. In den Gebäuden seien mehrere Kilometer Kupferkabel und Installation für Heizung und Sanitär verlegt, die es zu schützen gelte. Die Aufnahmen würden auf einer SD-Karte gespeichert und sollten bis zur Fertigstellung des Gebäudes aufbewahrt werden. Der TLfDI hatte noch einige Nachfragen. Zwischenzeitlich teilte der Bauherr mit, dass die Kamera abgebaut worden sei, weil der Bau fertiggestellt worden war. Auf Empfehlung des Architekten beabsichtigte der Bauherr jedoch, die aufgezeichneten Daten für eine eventuelle Baumängelverfolgung weiter aufzubewahren. Den entsprechenden Datenträger habe er in seinem Tresor hinterlegt. Somit sei sichergestellt, dass nur er Zugriff auf den Datenträger habe.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume mit Videoüberwachung nur dann zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegend schutzwürdiger Interessen der betroffenen Personen bestehen. § 6b Abs. 1 BDSG definiert die Videoüberwachung als Beobachtung mit optisch-elektronischen Einrichtungen. Von diesem Begriff werden nicht nur Videokameras erfasst, sondern auch Kameras, die in regelmäßigen Abständen Aufnahmen fertigen. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt. Nach dem Gesetzestext ist, bevor eine Videoüberwachung installiert wird, zu konkretisieren, welches Ziel damit erreicht werden soll. Ursprünglich verfolgte die verantwortliche Stelle hier den Zweck des Einbruchschutzes. Nunmehr sollte die nachträgliche Baumängelverfolgung ermöglicht werden. Gemäß § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu lö-

schen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Nach den von dem Betreiber übersandten Screenshots der Kameras war trotz der relativ geringen Auflösung der Bilder der Kamera nicht auszuschließen, dass auch personenbezogene Daten mit erfasst wurden. Auf den Aufnahmen waren die Nachbargebäude zu erkennen. Es war möglich, dort schemenhaft zu erkennen, ob sich eine Person auf dem Balkon aufhält oder nicht. Wenn man jedoch Zusatzwissen besitzt, beispielsweise wer in dieser Wohnung wohnt, war nicht auszuschließen, dass erkennbar war, wer sich jeweils auf dem Balkon aufhielt.
Dem Baustellenbetreiber wurde deutlich gemacht, dass die berechtigten Interessen der Anwohner einer längeren Speicherung der Aufnahmen entgegenstehen. Ansprüche auf die Beseitigung von Baumängeln verjähren erst nach fünf Jahren. Eine derartige Speicherdauer ist nach dem BDSG nicht zulässig. Da der TLfDI aber durchaus Verständnis für das Anliegen des Bauherren hatte, wurde folgende Vorgehensweise ausgehandelt: Der Bauherr verpflichtete sich, zur Baudokumentation jeweils nur ein Foto pro Tag zu sichern und sämtliche anderen Fotos zu löschen. Dabei musste er dafür sorgen, dass auf den verbleibenden Fotos keine personenbezogenen Daten zu erkennen waren, das heißt keine identifizierbaren Personen auf den Bildern zu sehen sind. Wenn auf den Fotos keine Personen mehr zu erkennen sind und damit keine personenbezogenen Daten verarbeitet werden, bedarf es für die Speicherung keiner gesetzlichen Grundlage, sie ist damit zulässig.

Auch das Anfertigen von digitalen Fotografien in relativ kurzen Zeitabständen unterfällt dem gesetzlichen Begriff der Videoüberwachung. Wenn auf den Fotos keine Personen oder sonstige personenbeziehbare Daten zu erkennen sind, können Fotos von Baustellen zur Dokumentation des Baufortschritts für längere Zeit gespeichert werden.

4.20 Baustellen-Webcam – Videogaga 19

Ein Bürger meldete sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und verwies auf eine Internetseite eines Thüringer Bauunternehmens. Dort konnte auf der Startseite von den Besuchern der Internetseite das Bild einer

Webcam zum Fortschritt einer Baustelle verfolgt werden. Bei so genannten Webcams handelt es sich um digitale Kameras, die bewegte oder unbewegte Bilder in das Internet übertragen. Dort können diese von jeder Internetnutzerin und jedem Internetnutzer eingesehen werden. Die Webcam war am Mast des Turmdrehkranes in einer Höhe von ca. 12 Metern installiert. Dabei aktualisierte sich das Bild der Webcam alle 5 Minuten automatisch. Es gab aber nach Aussage des Bauunternehmens zu keiner Zeit ein Livebild oder bewegte Bilder. Die Fotos der Kamera wurden direkt auf der Webseite dargestellt. Eine Speicherung oder Ähnliches erfolgte nach Auskunft des Bauunternehmens nicht. Nachdem der TLfDI ebenfalls die Internetseite aufrief, stellte er fest, dass das Bild der Webcam zu vergrößern war und eine recht hohe Auflösung aufwies. Die Webcam erfasste zum einen die Baustelle selbst, wobei auch Arbeitnehmer erfasst wurden, und zum anderen die umliegenden Grundstücke von Privathäusern, Gärten sowie Parkflächen. Es waren zwar keine Kraftfahrzeugkennzeichen zu lesen, ebenso waren die aufgenommenen Personen nicht direkt zu erkennen, allerdings war für den TLfDI nicht auszuschließen, dass mit einem gewissen Zusatzwissen die Autos und die erfassten Personen ohne Weiteres identifiziert werden konnten. Das Bauunternehmen teilte dem TLfDI mit, dass der Zweck der Webcam ausschließlich in der Werbung für das Bauunternehmen lag. Den Kunden und eventuellen Interessenten sollte mit der Webcam die kontinuierliche und organisierte Abwicklung der Baustelle näher gebracht werden. Weiterhin seien die Mitarbeiter über die Werbemaßnahme informiert gewesen.
Eine solche Übertragung von Bilddaten mittels einer Webcam kann nach Feststellung des TLfDI unter Umständen sowohl die Persönlichkeitsrechte der angrenzenden Nachbarn, als auch die Persönlichkeitsrechte der dort auf der Baustelle tätigen Beschäftigten verletzen. Problematisch ist in diesem Zusammenhang zudem, dass die Bilddaten mit ihrer Einstellung ins Internet einer unbestimmten Vielzahl von Personen weltweit zugänglich gemacht werden. Etwaige Persönlichkeitsrechtsverletzungen können aufgrund der technisch einfach zu handhabenden Möglichkeiten, die Bilder weiter zu verarbeiten und zu vervielfältigen, faktisch nicht mehr rückgängig gemacht werden („Das Internet vergisst nichts!“).
Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des Bundesdatenschutz-

gesetzes oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). § 6b Abs. 1 BDSG definiert die Videoüberwachung als Beobachtung mit „optisch-elektronischen Einrichtungen“. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Voraussetzung ist dabei jeweils die Erhebung personenbezogener Daten, das heißt, dass Personen auf den Aufnahmen erkennbar sein müssen oder sonst Rückschlüsse auf die Identität einer Person möglich sind. Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt. Damit unterfällt beispielsweise das Anfertigen von Fotos in kurzen Zeitintervallen ebenfalls der Vorschrift.
Solange nur Übersichtsaufnahmen angefertigt werden oder die Bilder so unscharf sind, dass eine Erkenn- und Identifizierbarkeit der abgebildeten Personen ausgeschlossen ist und auch keine anderen personenbezogenen Daten (wie zum Beispiel Kfz-Kennzeichen) erfasst und übermittelt werden, wird das Recht der Einzelnen auf informationelle Selbstbestimmung nicht berührt. Solche Webcams sind deshalb datenschutzrechtlich hinnehmbar. Allerdings sind Personen nicht nur dann identifizierbar, wenn ihre Gesichter zu erkennen sind, sondern beispielsweise auch bereits dann, wenn weitere Umstände wie etwa auffällige Kleidung, Frisur, Körpergröße, eine ersichtliche körperliche Behinderung oder ein bestimmtes Verhalten die Identifizierung einer Person ermöglichen. Dabei genügt es, wenn Menschen mit besonderem Zusatzwissen einzelne Personen auf den Bildern erkennen und identifizieren können. So können selbst dann, wenn die Bilder sehr unscharf oder grob aufgelöst sind, im Einzelfall gleichwohl noch einzelne Personen in ihren Datenschutzrechten verletzt sein. Insbesondere beim Einsatz von Webcams auf Baustellen ist zu berücksichtigen, dass durch Bildaufnahmen und -übertragungen ins Internet oftmals auch die Datenschutzbelange dort beschäftigter Personen betroffen sind. Sowohl durch Live-Übertragungen als auch durch Bilder, die im Minuten- oder Sekundentakt aktualisiert werden, können unter Umständen die Tätigkeit und Arbeitsweise von Beschäftigten über einen längeren Zeitraum via Internet verfolgt und kontrolliert werden. Selbst wenn die jewei-

ligen Beschäftigten durch technische Maßnahmen wie zum Beispiel Verpixelungen unkenntlich gemacht werden, besteht die Gefahr, dass beispielsweise Vorgesetzte ebenso wie Kolleginnen und Kollegen, die über das Zusatzwissen verfügen, welche Person zu welchem Zeitpunkt auf der Baustelle tätig ist, einzelne Beschäftigte via Internet bei ihrer Arbeit beobachten und permanent überwachen können. Ein solcher Einsatz von Webcams wäre deshalb aus Gründen des Beschäftigtendatenschutzes unzulässig.
Letztlich teilte das Bauunternehmen aber dem TLfDI mit, dass es nach Fertigstellung der Rohbauarbeiten den Baukran abgebaut hat. Deshalb sei die Kamera nun außer Betrieb genommen und demontiert. Jedoch plane man auch auf zukünftigen Baustellen wieder den Einsatz von Webcams zu Werbemaßnahmen. Der TLfDI empfahl dem Bauunternehmen für die Zukunft, das Zeitintervall, indem die Kamera die Fotos aufzeichnet, länger zu gestalten und die Fotos, bevor sie ins Netz gestellt werden, daraufhin zu überprüfen, ob tatsächlich keine Personen zu erkennen sind.

Bei der Anfertigung von reinen Übersichtsaufnahmen oder von unscharfen Bildern, auf denen keine Personen erkenn- und identifizierbar sind und auch keine anderen personenbezogenen Daten (wie zum Beispiel Kfz-Kennzeichen) erfasst und übermittelt werden, wird das Recht der Einzelnen auf informationelle Selbstbestimmung nicht berührt.

4.21 Die Zeitraffer-Kamera des Bauherren versus BDSG – Videogaga 20

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage einer Thüringer Film- und Fernsehproduktionsfirma zur Vereinbarkeit einer Zeitraffer-Kamera mit dem Bundesdatenschutzgesetz (BDSG). Das Thüringer Unternehmen erklärte, dass es die Kamera zur Aufnahme des Baufortschritts auf der Baustelle für ihre Auftraggeber installiert habe. In den dem TLfDI zur Verfügung gestellten Aufnahmen der Videokamera waren aber auch Häuser in der Nachbarschaft, deren Eingänge und Fenster zu erkennen. Zu einem wollte das Unternehmen die Aufnahmen zu Werbezwecken verwenden, zum anderen sollten die Aufnahmen für einen späteren Werbefilm der Auftraggeber angedacht sein. Technisch war nach Angaben des

Thüringer Unternehmens das System so aufgebaut, dass die Kamera alle fünf Minuten ein Standbild des Aufnahmebereichs erstellte. Die Bilder wurden ungefiltert angefertigt, d. h. ohne Schwärzungen oder Verpixelung. Im Nachhinein war von der Film- und Fernsehproduktion beabsichtigt, die kritischen Stellen per Unschärfe, Verpixeln oder Schwärzen unkenntlich zu machen.
Um das Ergebnis vorwegzunehmen: Die betriebene Zeitrafer-Kamera des Thüringer Unternehmens war mit dem BDSG nicht vereinbar. Dieses teilte der TLfDI dem Unternehmen mit.
Denn nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Es handelt sich also um ein Verbot mit Erlaubnisvorbehalt. Mit der Anfertigung der Bilder hat das Thüringer Unternehmen personenbezogene Daten erhoben, sodass es hier einer Ermächtigungsgrundlage bedurfte. Zwar beauftragt das BDSG den Landesgesetzgeber damit, für Pressearbeiten Ausnahmeregelungen zum BDSG zu schaffen, allerdings gelten diese Ausnahmen nur für Erzeugnisse, die ausschließlich zu eigenen journalistisch-redaktionellen Zwecken erhoben, verarbeitet oder genutzt werden, § 41 BDSG. Diesem Auftrag ist das Land Thüringen mit § 11a Thüringer Pressegesetz (TPG) auch nachgekommen. Diese ausschließlichen journalistisch-redaktionellen Zwecke waren im vorliegenden Fall nicht erkennbar. Hier sollten die Erzeugnisse auch zu werblichen bzw. gewerblichen Zwecken genutzt werden. Die Ausnahmeregelungen des TPG fanden daher auf dieses Vorhaben keine Anwendung. Auch Einwilligungen von allen in Frage kommenden Anwohnern im Sinne des § 4 Abs. 1 BDSG lagen dem Unternehmen nicht vor. Als gesetzliche Erlaubnisnormen kamen je nach Kameraeinstellung nur § 6b BDSG oder § 28 BDSG in Betracht. Die von dem Unternehmen dem TLfDI übersandten Beispielbilder der Zeitrafer-Kamera gaben öffentlich zugängliche Bereiche wieder. Insoweit war hier für die Beobachtung und Verarbeitung (Speicherung) der § 6b Abs. 1 Nr. 3, Abs. 3 BDSG einschlägig. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zu den optisch-elektronischen Einrichtungen zählen Geräte jeglicher Art und Gestal-

tung, die durch ein optisch-elektronisches Verfahren Licht in elektronische Signale umwandeln. Dabei ist es unerheblich, ob die Einrichtungen fest installiert oder mobil sind. Unbeachtlich ist auch, ob sie über eine Zoomfunktion oder eine Schwenkeinrichtung verfügen oder ferngesteuert werden können. Zu den optisch-elektronischen Einrichtungen gehören sowohl die analoge als auch die digitale Kameratechnik. Daher handelt es sich auch bei einer Zeitraffer-Kamera um eine optisch-elektronische Einrichtung im Sinne des § 6b Abs. 1 BDSG. Die Aufnahmen zu Werbezwecken und zur Darstellung des Baufortschritts stellten berechtigte Interessen des Thüringer Unternehmens dar und sind auch erforderlich. Allerdings stellte der TLfDI hier bei den Aufnahmen mit der Zeitraffer-Kamera ein Überwiegen der schutzwürdigen Interessen der Betroffenen fest, da ein relativ großer öffentlich zugänglicher Bereich beobachtet und von einer unbestimmbaren Anzahl an Betroffenen frequentiert wurde. Im Ergebnis waren daher die Aufnahmen unzulässig.
Soweit das Unternehmen nicht öffentlich zugängliche Bereiche aufgenommen hatte, kam eine Erhebungs- und Verarbeitungserlaubnis nur unter Maßgabe von § 28 Abs. 1 BDSG in Betracht. Die hierfür erforderlichen Voraussetzungen waren jedoch ebenfalls nicht gegeben. § 28 Abs. 1 BDSG erlaubt den Umgang mit personenbezogenen Daten unter speziellen Voraussetzungen für „die Erfüllung eigener Geschäftszwecke“. Selbst wenn man annahm, dass das Unternehmen mit den Auftraggebern – dem Architekten und Bauunternehmen – jeweils einen Werkvertrag über die Erstellung eines Werbefilms eingegangen war und damit zumindest eigene Geschäftszwecke vorlagen, rechtfertigte dies keinen Umgang mit personenbezogenen Daten nach § 28 Abs. 1 Nr. 1 BDSG, da kein Schuldverhältnis mit den Betroffenen (Nachbarn) bestand. Hinsichtlich § 28 Abs. 1 Nr. 2 BDSG ist zwar wie oben zu § 6b BDSG zuzugeben, dass ein berechtigtes Interesse besteht. Im Hinblick auf die grundrechtliche Stellung der Wohnung (vergleiche Art. 13 GG) bestand allerdings offensichtlich Grund zur Annahme, dass schutzwürdige Interessen Betroffener überwogen. Denn auf den übersandten Aufnahmen konnte der TLfDI erkennen, dass die Aufnahmen einen Einblick in die Fenster der Nachbarschaft ermöglichten. Ob diese im Nachhinein von dem Thüringer Unternehmen verpixelt wurden, hatte keinen Einfluss auf die rechtliche Bewertung.
Im Ergebnis gab es für den TLfDI keine anderen gesetzlichen Erlaubnisnormen zum Betreiben der Zeitraffer-Kamera. Eine daten-

schutzrechtliche zulässige Weiterführung der Aufzeichnung mittels einer Zeitraffer-Kamera wäre nur noch mit entsprechenden Einwilligungen der Betroffenen möglich gewesen. Diese Rechtsauffassung wurde der Thüringer Film- und Fernsehproduktion mitgeteilt, die sich daraufhin nicht mehr gemeldet hat.

Zu den optisch-elektronischen Einrichtungen im Sinne des § 6b Abs. 1 BDSG zählen Geräte jeglicher Art und Gestaltung, die durch ein optisch-elektronisches Verfahren Licht in elektronische Signale umwandeln. Dabei ist es unerheblich, ob die Einrichtungen fest installiert oder mobil sind. Unbeachtlich ist auch, ob sie über eine Zoomfunktion oder eine Schwenkeinrichtung verfügen oder ferngesteuert werden können. Zu den optisch-elektronischen Einrichtungen gehören sowohl die analoge als auch die digitale Kameratechnik.

4.22 Masse statt Klasse – Videogaga 21 – Vielzahl von Kameras in Unternehmen

Eine weitere Anfrage zur Zulässigkeit einer Videoüberwachung in einem Thüringer Unternehmen mit weit über 200 Kameras hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zum Anlass genommen, dies vor Ort zu überprüfen, zumal vorgetragen wurde, dass in der Vergangenheit Mitarbeiter unter Verweis auf die Kameraüberwachung gemaßregelt und entlassen worden wären.
Zunächst musste geklärt werden, inwieweit die Kontrollkompetenz des TLfDI gegeben war, da es sich bei dem Unternehmen um eine Niederlassung eines überregionalen Unternehmens handelte und der Sitz des Unternehmens nicht in Thüringen, sondern in einem anderen Bundesland lag. Die Zuständigkeit des TLfDI für die Niederlassung in Thüringen war nach § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz als Betriebsstätte in Thüringen gegeben. Allerdings muss in einem solchen Fall immer wieder geprüft werden, ob bestimmte Handlungen in der Verantwortung der Betriebsstätte oder des Hauptunternehmens liegen.
Die Vorortkontrolle ergab, dass circa 250 Kameras in und um die Betriebsstätte installiert waren. Die interne Verfahrensbeschreibung hierzu befand sich zu diesem Zeitpunkt in der Überarbeitung durch das Unternehmen. Eine Anlage zur Verfahrensbeschreibung, in der alle Kameras mit jeweiligem Standort aufgeführt sind, war ebenfalls

vorhanden, jedoch nicht ausreichend ausführlich, um eine datenschutzrechtliche Bewertung vornehmen zu können. Der jeweilige Zweck der Kameras war nur vereinzelt aus den Angaben ableitbar. Allgemein wurde der Zweck der Videoüberwachung mit der Zutrittsüberwachung, der Überwachung im technischen Bereich auch aus Gründen des Arbeitsschutzes und der Diebstahlsprävention bei hochpreisiger Ware angegeben.
Vor Beginn der Videoüberwachung ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen. Zudem sind technische und organisatorische Maßnahmen zu treffen (§ 9 Bundesdatenschutzgesetz [BDSG]), um die Sicherheit der Daten zu gewährleisten. Diesen Anforderungen genügten die im Unternehmen vorhandenen Unterlagen nicht.
Die einzelnen Kameras wurden in Augenschein genommen und der jeweilige Erfassungsbereich eingeschätzt. Dabei gab der TLfDI im Hinblick darauf, dass die Verfahrensbeschreibung ohnehin in Überarbeitung war, Hinweise zur zukünftigen Gestaltung der notwendigen technischen und organisatorischen Maßnahmen. Die Kameraüberwachung wurde nicht als insgesamt unzulässig eingestuft. Festgestellt wurde einerseits, dass die Kameras nicht offensichtlich darauf ausgerichtet waren, konkrete Arbeitsplätze und damit konkrete Beschäftigte zu überwachen. Dauerhaft eingerichtete Arbeitsplätze waren im Beobachtungsbereich regelmäßig nicht im Fokus bzw. es wurde der Aufnahmebereich abgedeckt beziehungsweise verpixelt. Übersichtsaufnahmen dienten insbesondere dem Arbeitsschutz. Bei der Vielzahl der Beschäftigten, die Warentransportfahrzeuge bedienten, die eine erhebliche Geschwindigkeit aufnehmen konnten, war verständlich, dass Unfälle und dergleichen im Nachhinein nachvollzogen werden müssen. Auch die Überwachung von technischen Anlagen zum Transport der Waren erschien erforderlich, um Havarien schnell zu bemerken und zu beseitigen. Pausen- oder Aufenthaltsräume für Beschäftigte waren von der Videoüberwachung ausgenommen.
Für die Kameras neben den Klingelanlagen zur Zutrittskontrolle reicht jedoch nach Auffassung des TLfDI regelmäßig Live-Monitoring als verlängertes Auge aus. Es ist grundsätzlich nicht erforderlich, aufzuzeichnen, wem Einlass gewährt wurde.
Werden Kameras innerhalb und außerhalb eines Gebäudes angebracht, reicht es nicht aus, am Eingang ein Schild mit der Aufschrift „Dieses Gebäude wird videoüberwacht“ aufzuhängen. Die Hinweis-

pflicht des § 6b Abs. 2 BDSG verlangt, dass auch die verantwortliche Stelle und der Umfang erkennbar gemacht wird, wenn nicht allein das Gebäude, sondern auch dessen Umgebung auf dem Grundstück des Unternehmens erfasst wird. Der Hinweis ist jeweils so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.
Die Hinweise des TLfDI während der Kontrolle vor Ort hat die Unternehmensleitung aufgenommen und deren Umsetzung angekündigt. Ein entsprechender Entwurf der internen Verfahrensbeschreibung liegt vor; angesichts der Vielzahl der zu überprüfenden Kameras ist die datenschutzrechtliche Bewertung noch nicht abgeschlossen.

Die Videoüberwachung in Unternehmen ist nicht an sich unzulässig. Es kommt darauf an, aus welchen Gründen überwacht wird und ob die videoüberwachten Bereiche über das gebotene Maß hinausgehen. Mitarbeiterarbeitsplätze dürfen nicht so erfasst werden, dass ein Mitarbeiter seine ganze Schicht vor der Videokamera verbringen muss. Bei einer Kontrolle prüft der TLfDI jede Kamera einzeln auf ihre datenschutzrechtliche Zulässigkeit.

4.23 Ein Häuschen steht am Walde – kein Videogaga 22

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass ein Einwohner einer abgelegenen 200-Seelen-Gemeinde mithilfe von drei Videokameras den Eingangsbereich seines Wohnhauses sowie ein Stück des angrenzenden Gehweges überwachte. Die Nachbarn fühlten sich gestört. Der TLfDI informierte den Betreiber der Videoüberwachung in seinem ersten Anschreiben darüber, dass das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig ist, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des Bundesdatenschutzgesetzes oder der Betroffene hat in den Vorgang eingewilligt (das so genannte Verbot mit Erlaubnisvorbehalt). Um beurteilen zu

können, inwieweit die von ihm betriebenen Kameras mit dem BDSG in Einklang zu bringen waren, forderte der TLfDI ihn auf, einen Fragenkatalog zu seiner Videoüberwachung zu beantworten. Die Fragen waren so zu beantworten, dass die Antworten den Zustand der Videoüberwachung zum Zeitpunkt des Zugangs seines Schreibens widerspiegelten. Die Auswertung der Antworten und des ebenfalls angeforderten Bildmaterials ließen keinen Verstoß gegen das Bundesdatenschutzgesetz erkennen. Die drei Kameras waren nur auf das eigene Grundstück gerichtet und nicht schwenkbar. Gegen diese Praxis war in dem Fall aus datenschutzrechtlicher Sicht nichts einzuwenden.

Bei der Installation von Anlagen der Videoüberwachung auf einem Privatgrundstück muss sichergestellt sein, dass weder der angrenzende öffentliche Bereich noch benachbarte Privatgrundstücke oder der gemeinsame Zugang zu diesen von den Kameras erfasst werden, sofern nicht ein das Persönlichkeitsrecht der Betroffenen überwiegendes Interesse des Betreibers der Anlage im Rahmen der Abwägung bejaht werden kann. Darüber hinaus kommt es darauf an, wie das eigene Grundstück gestaltet ist. Sollen hier regelmäßig Dritte Zutritt haben, kann auch auf dem eigenen Grundstück eine Videoüberwachung unzulässig sein. Denn auch Privatgrundstücke können öffentlich zugängliche Räume sein. Hier ist eine Videoüberwachung dann nur nach Maßgabe des § 6b BDSG zulässig.

4.24 Garagenkino – Videogaga 23

Kameraattrappen waren schon mehrfach Thema in diesem 2. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zum nicht-öffentlichen Bereich. So erreichte den TLfDI auch ein Hinweis einer Stadtverwaltung. Ein Eigentümer einer Garage setzte die Stadtverwaltung darüber in Kenntnis, dass in einer Garagengemeinschaft ein Garagenbesitzer eine Videokamera an der Außenfassade seiner Garage installiert hatte. Darüber hinaus teilte die Stadtverwaltung dem TLfDI mit, dass sämtliche Garagen und Zufahrtsflächen zu den Garagen sich in Privatbesitz befänden, der Zugang zu diesen aber nicht verwehrt sei. Weiterhin befand sich an der Zufahrt zur Garagengemeinschaft ein Schild mit der Aufschrift „Privatgrundstück. Betreten verboten“.

Zunächst musste der TLfDI den Betreiber der installierten Kamera ermitteln. Dieser teilte sodann mit, dass es sich bei der Videoüberwachungsanlage um eine Kameraattrappe handelte. Eine Kameraattrappe erhebt zwar keine personenbezogenen Daten, jedoch geht von solchen derselbe Überwachungsdruck wie von richtigen Kameras aus. Die betroffenen Personen wissen ja nicht, ob sie aufgezeichnet werden oder nicht. Daher werden solche Attrappen vom TLfDI genauso behandelt wie funktionstüchtige Kameras. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Danach ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung durch nicht-öffentliche Stellen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Auf diesen Umstand wurde der Betreiber, eine Privatperson, vom TLfDI hingewiesen. Der Betreiber zeigte sich einsichtig und teilte dem TLfDI mit, dass er die Attrappe entfernt habe. Daraufhin hat der TLfDI die Stadtverwaltung Walterhausen im Rahmen der Amtshilfe gemäß § 4 Abs. 1, § 5 Abs. 1 Nr. 3 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) gebeten, zu kontrollieren, ob die Attrappe wirklich entfernt wurde. Sobald die Stadtverwaltung dem TLfDI dieses bestätigt, ist das Verfahren beendet.

Der Zustand, ob es sich um eine echte Videokamera oder um eine Attrappe handelt, ist von außen nicht erkennbar, womit der Überwachungsdruck für den Betroffenen gleich bleibt. Daher müssen auch Attrappen die Voraussetzungen des § 6b BDSG sinngemäß erfüllen, um zulässig zu sein.

4.25 Videoüberwachung durch Grundstücksnachbarn – Videogaga 24

Das Filmen ist noch nicht vorbei. Erneut erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über die Installation einer Videokamera durch einen Nachbarn. Der Beschwerdeführer teilte dem TLfDI mit, dass die Kamera auf dem Privatgrundstück des Nachbarn installiert

sei. Darüber hinaus sei diese auf die angrenzenden öffentlichen Wege ausgerichtet.
Wie schon mehrfach in diesem Tätigkeitsbericht darüber informiert wurde, ist maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage, die öffentlich zugängliche Räume erfasst, § 6b BDSG. Bei öffentlich zugänglichen Räumen handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen.
Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Darüber hinaus ist vor Beginn der Videoüberwachung konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall diesen soll. Dabei ist der Überwachungszweck bei mehreren Kameras für jede einzeln gesondert und konkret anzugeben. Schließlich müssen die Kameras für diesen festgelegten Zweck geeignet und erforderlich sein. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann (Beispiel: Umzäunung, regelmäßige Kontrollgänge, Sicherheitsschlösser usw.). Auch eine Überwachung nur in den Nachtstunden oder außerhalb von Geschäftszeiten kann im Gegensatz zu einer dauerhaften Überwachung ausreichend sein.
Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Inte-

ressen der Betroffenen nicht überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Maßstab der Bewertung ist das informationelle Selbstbestimmungsrecht als besondere Ausprägung des Persönlichkeitsrechts auf der einen und der Schutz des Eigentums oder der körperlichen Unversehrtheit auf der anderen Seite.
Vorliegend war die Videoüberwachung auf einen öffentlich zugänglichen Weg, der regelmäßig als Zuweg zu einem Hotel genutzt wurde, ausgerichtet. Der TLfDI schrieb den angeblichen Betreiber mit der Bitte um Stellungnahme an. Daraufhin teilte der angebliche Betreiber dem TLfDI mit, dass er keine Kamera betreibe. Nach glaubhaften Informationen des TLfDI war das Gegenteil der Fall. Es wird daher zunächst im Rahmen eines Amtshilfeverfahrens das dortige Ordnungsamt gebeten werden, den Sachstand zu ermitteln und zu dokumentieren. Sollten sich die Kamera, ihr Standort und die Ausrichtung bestätigen, wird der TLfDI nach Prüfung deren Zulässigkeit aller Wahrscheinlichkeit nach die Demontage anordnen und ein Bußgeldverfahren einleiten.

Die Beurteilung der datenschutzrechtlichen Zulässigkeit von Kameras kann rechtlich komplex sein, da die rechtliche Einordnung von unterschiedlichen Umständen des Einzelfalls abhängig ist. Verantwortlich für diese Beurteilung ist immer der Betreiber der Kamera(s) selbst. Stellt der TLfDI fest, dass die datenschutzrechtlichen Voraussetzungen nicht erfüllt sind und die Videoüberwachung daher unzulässig ist, drohen eine Abbauanordnung sowie ein Bußgeldverfahren.

4.26 Einfamilienhaus mit Rundumblick? – Videogaga 25

In einem kleinen Ort in Thüringen wurde im Berichtszeitraum ein Nachbarschaftsstreit ausgetragen, wie er im Buche steht. Hauptsächlich wurden Sachbeschädigungen, die Nachbar A begangen hatte, vom Nachbarn B festgestellt und nachgewiesen. Nun ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) aber nicht dafür zuständig, Nachbarschaftsstreitigkeiten zu schlichten, sondern um Datenschutzverstöße festzustellen und gegebenenfalls zu ahnden. Zum Beispiel, wenn es um Videotechnik geht, die auch hier zum Einsatz kam. Nachbar A hatte sich über Nachbar B beschwert, weil der angeblich die Straße und die Nach-

barschaft von seinem Haus rundum überwachte. Nach der Prüfung des TLfDI wurde festgestellt, dass Nachbar B zwar funktionstüchtige Kameras angebracht hatte, diese aber zum Schutz seines Eigentums erforderlich waren und keineswegs die gesamte Nachbarschaft überwachten. Die Kameras waren tagsüber abgeschaltet und nur in den Nachtstunden in Betrieb. Der Erfassungsbereich der Kameras beschränkte sich „nur“ auf das eigene Grundstück und einen kleinen Streifen vor dem Haus. Dort wurde das Fahrzeug der Familie abgestellt. Insbesondere wurde der Hof der Familie überwacht, weil dort vom Nachbargrundstück Bauschutt verteilt wurde.

Gegenstand der Erforderlichkeitsprüfung einer Videoüberwachungsanlage muss nicht nur das „Ob“, sondern auch und vor allem das „Wie“ eines Einsatzes von Videotechnik sein. Hierbei sind insbesondere der zeitliche und räumliche Umfang sowie die organisatorische Ausgestaltung zu berücksichtigen (Scholz in Simitis, Bundesdatenschutzgesetz, 8. Aufl., § 6b, Rn. 89). Die Beobachtung „öffentlich zugänglicher Räume“ wird in § 6b Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) geregelt und ist nur zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der von der Videoüberwachung betroffenen Personen überwiegen. Die Eigentumsverhältnisse am Beobachtungsobjekt sind für die Erfüllung dieses Tatbestandsmerkmals allerdings unbeachtlich. Die streitgegenständliche Kamera wurde ausschließlich zur Gefahrenabwehr und Eigentumssicherung betrieben. Somit beschränkte sich der Verwendungszweck auf den Schutz eigener Rechtsgüter des Nachbarn B. Darüber hinaus hat das Amtsgericht Berlin-Mitte am 18. Dezember 2013 (Aktenzeichen 16 C 427/02) entschieden, dass eine Videoüberwachungsanlage im öffentlich zugänglichen Raum einen ein Meter breiten Streifen entlang der Straßenseite sowie einen ein Meter breiten Streifen links und rechts der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen darf. Danach bleibt eine einmal zulässige Videoüberwachung nicht automatisch für immer rechtmäßig. Die Umstände, die zu ihrer Rechtmäßigkeit geführt haben, sind vielmehr in angemessenen Abständen vom TLfDI zu prüfen. Sollten die Blickwinkel der Kameras neu ausgerichtet werden, muss der TLfDI die Videoüberwachungsanlage erneut datenschutzrechtlich bewerten.

Nach Prüfung des Sachverhaltes war die Videoüberwachung vor Ort als zulässig zu bewerten. Die Ausgestaltung der Überwachung war

hinsichtlich der erfassten öffentlich zugänglichen Räume unter Berücksichtigung von § 6b BDSG so vorgenommen, dass sie dem Schutzbedürfnis der Betroffenen ausreichend Rechnung trägt (s a. Urteil des Bundesgerichtshofs Az. V ZR 220/12 vom 24. Mai 2013). Eine erneute Überprüfung der Erforderlichkeit im Hinblick auf die äußeren Umstände wird vom TLfDI im Jahr 2016 vorgenommen.

Eine überprüfte und für zulässig gehaltene Kamera kann im Einzelfall mit Zeitablauf ihre Erforderlichkeit verlieren. Insbesondere dann, wenn sich die äußeren Umstände, die Anlass zur Videoüberwachung gegeben haben, ändern. Daher ist die Zulässigkeit von Kameras durch die verantwortliche Stelle in regelmäßigen Abständen zu überprüfen. Gegebenenfalls sind dann Änderungen vorzunehmen.

4.27 Grundrechtseingriff durch Attrappe – Videogaga 26

Aufgrund eines Hinweises erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, dass eine Hauseigentümerin eine Videokamera an ihrem Haus unterhalb der Dachrinne angebracht hatte. Auf Nachfrage bei der Hauseigentümerin, teilte diese dem TLfDI mit, dass es sich bei der von ihr angebrachten Kamera lediglich um eine Attrappe und nicht um eine echte Kamera handelte. Die Attrappe, welche auf das große Schaufenster im Erdgeschoss gerichtet war, setzte die Hauseigentümerin zum Schutz vor Vandalismus und damit zur Abschreckung von gewaltbereiten Tätern ein. Gerade dafür sei es nach Aussage der Hauseigentümerin erforderlich gewesen, dass die Dummy-Kamera einer echten täuschend ähnlich sah. In der Vergangenheit sei bereits das Auto des gegenüber wohnenden Nachbarn der Hauseigentümerin mit einem Stein stark beschädigt und eine Steinmauer auf der gegenüberliegenden Straßenseite mit Graffiti besprüht worden.
Die Beurteilung der datenschutzrechtlichen Zulässigkeit von Videokameras in Wohnbereichen ist schwierig und hängt von unterschiedlichen Umständen des Einzelfalls ab. Nach dem Willen des Gesetzgebers muss die in weiten Bereichen von öffentlichen und nichtöffentlichen Stellen bereits durchgeführte Videoüberwachung öffentlich zugänglicher Räume, wie auch im vorliegenden Fall, auf eine gesetzliche Grundlage gestützt werden, die der Wahrung der informationellen Selbstbestimmung durch einen angemessenen Interessenausgleich Rechnung trägt. Handelt es sich also bei dem über-

wachten „Raum“ um einen öffentlich zugänglichen Bereich, regelt § 6b Bundesdatenschutzgesetz (BDSG) die datenschutzrechtliche Zulässigkeit. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen endet. Wer außerhalb seines Grundstücks auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mitüberwacht werden. Jedoch lässt die Rechtsprechung je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter aufgenommen wird. Auch im vorliegenden Fall schloss der TLfDI bei der Ausrichtung der Kameraattrappe auf das große Schaufenster im Erdgeschoss ein Erfassen von öffentlich zugänglichem Raum nicht aus.

Schließlich behandelt der TLfDI Kameraattrappen genauso wie das funktionierende Modell, weil der Eingriff in die Grundrechte der Betroffenen nahezu identisch ist. Daher findet das BDSG nach Auffassung des TLfDI auch bei Videoüberwachungsanlagen, die nicht im Betrieb sind, und auf Videokameraattrappen Anwendung. Mit dem Einsatz von Kameraattrappen ist ein Eingriff in das allgemeine Persönlichkeitsrecht verbunden, denn die Kameraattrappe soll bei den Betroffenen die Vorstellung einer funktionsfähigen Anlage erzeugen, um sie von einem unerwünschten Verhalten abzuhalten. Gerade von Kameraattrappen, die aus objektiver Sicht den Anschein der Echtheit erwecken, geht derselbe Anpassungs- und Überwachungsdruck wie von funktionstüchtigen Kameras aus. Die Aufstellung einer solchen Attrappe stellt für den Betroffenen die dauernde Androhung einer Videoüberwachung dar. Die betroffene Person sieht sich damit in jedem Fall einer Kontrollmöglichkeit ausgesetzt. Die unbefangene, von Zwangswirkungen freie Kommunikation,

Interaktion und Darstellung in der Öffentlichkeit ist aber Grundbedingung für die freie Entfaltung der Persönlichkeit.
Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit.
Im vorliegenden Fall konnte die Hauseigentümerin nicht nachweisen, dass im Vorfeld durch wiederholten Vandalismus und ähnliche Vorkommnisse zu ihren Lasten Schäden an ihrem Eigentum entstanden sind, die auch eine echte Kamera zur Wahrnehmung berechtigter Interessen rechtfertigen würden. Vielmehr war nur die Rede von Vorkommnissen in der Nachbarschaft. Die im Einsatz befindliche Videoattrappe an der Dachrinne des Hauses, mit Ausrichtung auf öffentlich zugänglichen Raum, ist daher nach derzeitiger Aktenlage wegen Anhaltspunkten, dass schutzwürdige Interessen der Betroffenen überwiegen, unzulässig. Das Verfahren ist noch nicht abgeschlossen. Der TLfDI wird die Hauseigentümerin auffordern, die Kameraattrappe zu demontieren oder anders auszurichten.

Auch bei der Verwendung von Attrappen ist zu prüfen, ob die datenschutzrechtlichen Vorgaben eingehalten werden oder nicht. In allen Bereichen, in denen sich danach der echte Kameraeinsatz verbietet, würde somit auch der Einsatz von Kamera-Attrappen einen Rechtsverstoß bedeuten.

4.28 Fachwerkhaus mit neuer Technik – Videogaga 27

Im Berichtszeitraum übermittelte eine Thüringer Polizeiinspektion dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Angelegenheit zur möglichen

Verfolgung eines datenschutzrechtlichen Verstoßes. Die Polizeiinspektion teilte mit, dass ihre Polizeibeamten an der Außenfassade eines Fachwerkhauses eine Kamera festgestellt hätten. Die Kamera habe für die Polizeibeamten den Anschein erweckt, dass sie in Betrieb sei. Der TLfDI nahm sich der Angelegenheit an und hat daraufhin zunächst versucht, den Eigentümer des Fachwerkhauses zu ermitteln. Dazu bat er das zuständige Grundbuchamt im Rahmen der Amtshilfe nach § 4 Abs. 1 Thüringer Verwaltungsverfahrensgesetz um Auskunft über den Eigentümer des Fachwerkhauses. Nach Mitteilung des Eigentümers vom Grundbuchamt schrieb der TLfDI den Eigentümer des Fachwerkhauses mit der Bitte um Auskunft zu den gestellten Fragen an. Daraufhin leitete die Vermieterin als Eigentümerin des Fachwerkhauses das Auskunftsverlangen des TLfDI im Sinne des § 38 Abs. 3 Bundesdatenschutzgesetz an ihre Mieterin als Betreiberin der streitgegenständlichen Kamera weiter. Die Mieterin antwortete dem TLfDI, dass sie am Dachkasten lediglich eine Kameraattrappe installiert habe. Diese sei weder in der Lage, Videos aufzuzeichnen noch Fotos zu schießen. Sie diene lediglich der Abschreckung. Da von Seiten der Nachbarn ständig Fragen dazu kämen, habe sie die Kameraattrappe wieder entfernt.

Wie schon mehrfach in diesem Tätigkeitsbericht ausgeführt, sind die Vorschriften des BDSG auch auf Kameraattrappen anzuwenden, weil der durch die Attrappe ausgelöste Überwachungsdruck dem einer funktionsfähigen Kamera entspricht (vergleiche dazu Beitrag 4.27). Hierdurch wird ein ähnlicher Eingriff in das Grundrecht der informationellen Selbstbestimmung vorgenommen wie durch eine tatsächlich funktionierende Kamera. Eine Überwachung im privaten Bereich, wie hier am Dachkasten des Fachwerkhauses, ist nur unter bestimmten Umständen rechtlich zulässig. Insofern ist auch bei Verwendung von Attrappen zu prüfen, ob die datenschutzrechtlichen Vorgaben zur Beobachtung öffentlich zugänglicher Räume nach § 6b BDSG eingehalten werden.

Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welcher die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Nicht-öffentliche Stellen sind private Betreiber von Videotechnik, z. B. Unternehmen oder Privatpersonen, wie hier die Mieterin des Fachwerkhauses.

Mit der Mitteilung der Mieterin, dass sie die Kameraattrappe entfernt habe, konnte der TLfDI das Verfahren abschließen.

Die Installation von Videokameras als auch die Installation von Kameraattrappen an Gebäuden stellt einen Eingriff in die Rechte der Mieter, der Anwohner, Besucher und anderer Betroffener dar. Allein schon durch die Attrappe befinden sich die Betroffenen unter dem Eindruck ständiger Überwachung.

4.29 Das elektronische Auge in der Nachbarschaft – Videogaga 28

Und wieder einmal lag dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Prüfung der Sach- und Rechtslage die Beschwerde eines Bürgers über dessen Nachbarn vor. Die Nachbarn sollen im Fenster ihres Erdgeschosses eine Kamera, ausgerichtet auf den öffentlichen Verkehrsausraum, angebracht haben.
Daraufhin schrieb der TLfDI die Nachbarn mit der Bitte um Stellungnahme mit seinem umfassenden Fragenkatalog an. Die Nachbarn teilten dem TLfDI mit, dass sie niemals eine Videoüberwachungsanlage betrieben hätten, denn die Kamera wäre zu keiner Zeit eingeschaltet gewesen. Die nicht funktionstüchtige Kamera sollte lediglich der Abschreckung dienen.
Wie bereits schon mehrfach in diesem Tätigkeitsbericht aufgezeigt, stellt auch eine nicht funktionstüchtige Kamera oder eine Kameraattrappe ein erhebliches datenschutzrechtliches Problem dar, da Nachbarn, Passanten und sonstige Verkehrsteilnehmer nicht wissen können, dass hinter der Kamera kein Beobachtungs- bzw. Aufzeichnungssystem steckt. Daher entwickelt eine Kameraattrappe oder eine nicht funktionstüchtige Kamera den gleichen Überwachungsdruck wie ein funktionierendes Modell, da gerade eine Videobeobachtung suggeriert werden soll. Wegen dieses gleichen Beobachtungsdrucks sind auch Attrappen nur unter denselben Bedingungen zulässig, die eine echte Kamera an Stelle der Attrappe erfüllen müsste. Daher sind auch die Vorschriften des Bundesdatenschutzgesetzes (BDSG) auf Kameraattrappen anzuwenden. Insofern prüft der TLfDI bei Verwendung von Attrappen, ob die datenschutzrechtlichen Vorgaben zur Beobachtung öffentlich zugänglicher Räume nach § 6b BDSG eingehalten werden. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welcher die Videoüberwachung von öffentlich zugänglichen Räumen durch

nicht-öffentliche Stellen regelt. Nicht-öffentliche Stellen sind private Betreiber von Videotechnik, z. B. Unternehmen oder Privatpersonen. Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich um Bereiche, die dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können, ohne dass es darauf ankommt, ob es sich um einen umschlossenen oder überdachten Bereich handelt. Bei einem angrenzenden Gehweg wie hier handelt es sich um solch einen öffentlich zugänglichen Raum.
Das Verfahren ist noch nicht abgeschlossen. In der Stellungnahme zum Fragenkatalog führten die Nachbarn aus, dass sie die nicht funktionstüchtige Kamera mittlerweile abgebaut hätten. Dies wird der TLfDI überprüfen. Sollte sich dieses bestätigen, kann das Verfahren abgeschlossen werden.

Auch nicht funktionstüchtige Kameras sind grundsätzlich nach den gleichen Maßstäben zu beurteilen wie die tatsächlich funktionsfähigen Kameras, da von einem nicht funktionstüchtigen Modell der gleiche Überwachungsdruck ausgeht.

4.30 Leuchtende Kamera – kein Videogaga 29

Immer diese Nachbarn. Eine Familie fühlte sich durch den Nachbarn belästigt, weil dieser wohl die einzige Zufahrt zu ihrem Grundstück mit zwei Kameras videografierte. Die Kameras seien am Dach des Carports der Familie angebracht. Ein Hinweisschild war nicht zu sehen.
Die Erhebung von Videoaufnahmen bedarf nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) einer gesetzlichen Ermächtigung oder der Einwilligung aller gefilmten Personen. Der Natur der Sache nach kommt bei einer Videoüberwachung aufgrund der unbestimmten Anzahl videografierter Personen keine Einwilligungslösung in Betracht. Vielmehr bedarf es einer gesetzlichen Grundlage. In diesem Fall ist § 6b des Bundesdatenschutzgesetzes (BDSG) die einschlägige Norm. Zur Bewertung der Videoüberwachungsanlage wandte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Auskunftsersuchen nach § 38 Abs. 3 BDSG an den Nachbarn. Dieser teilte sehr schnell mit, dass keine Kameras angebracht seien. Es handele sich vielmehr

um eine Solarleuchte, die bei Dunkelheit anspringt und das Carport des Nachbarn sowie dessen Privatweg hin zu seinem Hauseingang bei Dunkelheit ausleuchtete. Der Nachbar wies die Solarleuchte mit eindeutigen Bildern und einem Kassenzettel nach. Damit war das BDSG offensichtlich nicht anwendbar und der TLfDI nicht zuständig. Dem Beschwerdeführer wurde mitgeteilt, dass es sich nicht, wie von ihm vermutet, um eine private Videoüberwachung des öffentlichen Raums handelte, sondern vielmehr um eine Form der Beleuchtung durch zwei Solarleuchten.

Oftmals sehen Solarleuchten und deren Bewegungsmelder wie Kameras aus. Eine Videoüberwachung liegt nur vor, wenn eine Datenerhebung durch eine Beobachtung mit elektronischen Einrichtungen vorgetäuscht (Kameraattrappe) wird oder tatsächlich stattfindet.

4.31 Radelnder Filmer – Videogaga 30

Ein Mieter beschwerte sich darüber, dass ihn die Nachbarn auf dem Balkon fotografieren würden. Hinzu kam auch noch, dass der Nachbar ihm und seiner Frau bei einem Ausflug in die Stadt mit dem Rad folgte und ein Video mit seinem Smartphone drehte.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen, Privatpersonen) regelt das Bundesdatenschutzgesetz (BDSG), soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben, § 1 Abs. 2 BDSG. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat hingegen keine Zuständigkeit inne, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 (C 212/13) ist diese Regelung allerdings eng auszulegen. Wie in der Pressemitteilung des TLfDI „Weihnachtsgeschenk für den Datenschutz!“ (Anlage 19)] bekannt gegeben, ist entscheidend, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen videoüberwacht werden, die mit dem Videobetreiber nicht in einer persönlichen Nähebeziehung stehen. Dies gilt in diesem Fall

insbesondere auch für die Bildaufnahmen der Nachbarbalkone. Das BDSG war im vorliegenden Fall also anwendbar.
Weiterhin ist nach § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Nach § 4a BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Hinsichtlich der grundsätzlichen Schriftform der Einwilligung im Datenschutzrecht werden an die Einwilligung zur Erstellung von Fotos und Videos geringere Anforderungen gestellt. Die Einwilligung muss nicht ausdrücklich, sondern kann unter bestimmten Voraussetzungen auch konkludent erteilt werden. Wer zum Beispiel fotografiert/gefilmt wird und in die Kamera winkt, erklärt durch sein Handeln regelmäßig, dass er damit einverstanden ist und gibt dem Fotografierenden somit eine konkludente Einwilligung. Dies funktioniert selbstverständlich nur dann, wenn dem Fotografen nichts Gegenteiliges bekannt ist. Als in diesem Fall dem Betroffenen auffiel, wie sich der Nachbar auf dem Fahrrad näherte und ein Video aufnahm, drehte er sich augenblicklich wieder um. Hierunter ist definitiv keine Einwilligung zu sehen. Wegen der fehlenden Einwilligung des Betroffenen bedurfte es einer gesetzlichen Grundlage. Nach § 6b Abs. 1 BDSG ist die Videoüberwachung nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Diese Voraussetzungen waren alle nicht gegeben. Der Nachbar war keine öffentliche Stelle noch hätte er mit dem Filmen seines Nachbarns vom Fahrrad sein Hausrecht wahrnehmen können. Ein anderes berechtigtes Interesse des Nachbarn konnte ebenfalls nicht festgestellt werden. Jedenfalls hätte das Interesse des Betroffenen am Ausschluss einer Videoüberwachung ein Interesse des radelnden Nachbarn überwogen. Der gefilmte Nachbar wurde vom TLfDI auch darüber informiert, dass er parallel zivilrechtliche Unterlassungs- und Abwehransprüche geltend machen könne, § 823 i. V. m. § 1004 BGB.
Der TLfDI ermittelt gerade eine zustellfähige Anschrift, um diese Rechtsauffassung mitzuteilen; die filmende Person ist allem Anschein nach unbekannt verzogen.

Betroffene einer Videoüberwachung haben nicht nur die Möglichkeit, sich an die zuständige Aufsichtsbehörde für den Datenschutz zu wenden. Sie können auch zivilrechtliche Unterlassungs- und Abwehransprüche gegen den Verantwortlichen der Videoüberwachung geltend machen.

4.32 "Ob ihr wirklich richtig steht, seht ihr, wenn die Kamera angeht." – Videogaga 31 – Videoüberwachung durch Nachbarn

Gegenstand einer Beschwerde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) waren erneut Videoaufnahmen vom Nachbarn. Bei der betriebenen Videoüberwachungsanlage handelte es sich um insgesamt vier Funkkameras auf einem eingezäunten Privatgrundstück. Nachdem der TLfDI den Nachbarn mit der Bitte um Auskunft nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) angeschrieben hatte, überreichte dieser Standortfotos der Kameras sowie Screenshots der jeweiligen Aufnahmebereiche der vier Funkkameras.
Grundsätzlich findet das Bundesdatenschutzgesetz (BDSG) auf jeden Umgang mit personenbezogenen Daten Anwendung, vergleiche § 1 Abs. 1 BDSG. Gerade bei Videoüberwachungen werden personenbezogene Daten erhoben und gegebenenfalls gespeichert. Einziger Ausschlussgrund für nicht-öffentliche Stellen stellt die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten für ausschließlich persönliche oder familiäre Tätigkeiten dar, § 1 Abs. 2 Nr. 3, 2. Hs BDSG. Der Ausschlussgrund der persönlichen oder familiären Tätigkeit ist nur dann gegeben, wenn der Umgang mit den personenbezogenen Daten ausschließlich innerhalb der persönlichen oder familiären Sphäre (z. B. Grundstück, Familienangehörige) desjenigen vorgenommen wird, der die Daten verarbeitet (also erhebt, speichert, nutzt etc.).
In einer am 11. Dezember 2014 ergangenen Entscheidung hat der Europäische Gerichtshof (EuGH, Urteil vom 11. Dezember 2014, C212/13) klargestellt, dass jede Videoüberwachung, die **nicht ausschließlich auf die private Sphäre** (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie öffentlich zugänglichen Raum oder Nachbargrundstücke erfasst, in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des gleichlautenden Bundesdatenschutzgesetzes (BDSG) fällt.

Die Videoüberwachung ist damit nur unter den dort geregelten Voraussetzungen zulässig.
Im konkreten Fall stellte der TLfDI fest, dass die Videoaufnahmen von dem Nachbarn lediglich den privaten Bereich betrafen und zu ausschließlich privaten Zwecken erfolgten, weswegen eine Zuständigkeit des TLfDI nicht gegeben war.

Die datenschutzrechtlichen Grenzen sind spätestens seit der Grundsatzentscheidung des EuGH vom 11. Dezember 2014 (Az.: C212/13) auch bei der privaten Videoüberwachung zu beachten, wenn diese den privaten/familiären Raum verlässt. Nicht unter den Anwendungsbereich des BDSG fällt die Videoüberwachung für ausschließlich persönliche oder familiäre Tätigkeiten.

4.33 Empörung in der Nachbarschaft – Videogaga 32

Ein Bewohner einer kleinen Stadt in Thüringen trat im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran und machte darauf aufmerksam, dass die Straße und Buswendeschleife videoüberwacht werde. Auch angrenzende Nachbarn seien von der Videoüberwachung betroffen. Die Anwohner waren über die Kamera empört. Zumal sie nicht wussten, ob neben Bild- auch Tonaufzeichnungen gefertigt wurden.
Der vermeintliche Betreiber der Videokamera wurde zunächst vom TLfDI mit einem umfangreichen Fragenkatalog zur Überwachung der Straße und der Wendeschleife befragt. Als dieser mitteilte, dass er keine Kamera installiert hatte, forderte der TLfDI Bilder über die angezeigte Videokamera vom Beschwerdeführer. Die Bilder vom Beschwerdeführer wurden bis zum Ende des Berichtszeitraums nicht geliefert. Vielmehr teilte er dem TLfDI mit, der Kamerabetreiber habe die streitgegenständliche Kamera nunmehr mit Kabeln versehen. Weiterhin wurde mitgeteilt, dass die Kamera mit einem Bewegungsmelder versehen worden sein musste. Diese bewege sich mit in Richtung der davor stehenden Person.
Dennoch ist nach § 4 Abs. 1 BDSG eine Videoüberwachung, wie jeder Umgang mit personenbezogenen Daten, grundsätzlich unzulässig, es sei denn es gibt eine gesetzliche Erlaubnis innerhalb oder außerhalb des Bundesdatenschutzgesetzes (BDSG) oder es liegt eine Einwilligung aller gefilmten Personen vor. Ist keine der beiden Vo-

raussetzungen gegeben, so ist die Videoüberwachung unzulässig. Eine Einwilligung kam der Natur der Sache nach nicht in Betracht. Es kam also nur eine Zulässigkeit aufgrund einer Erlaubnisnorm in Betracht.

Als Erlaubnisnorm kam nur der § 6b BDSG in Frage. Demnach ist eine Videoüberwachung in einem öffentlich zugänglichen Raum nur zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Um ein berechtigtes Interesse an einer Videoüberwachung zur Wahrnehmung des Hausrechts und zur Aufklärung von Straftaten zu sehen, muss eine tatsächliche Gefahrenlage nachgewiesen werden. Die Videoüberwachung muss insbesondere auch erforderlich sein, um den verfolgten Zweck zu erreichen. Jedenfalls muss abgewogen werden, ob es Alternativen zur Zweckerreichung gibt, die weniger in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreifen.

Selbst wenn eine Videoüberwachung erforderlich wäre, kann sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffen überwiegen. Eine permanente Überwachung, der eine betroffene Person nicht ausweichen kann, stellt einen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dies wäre bei einer dauerhaften Überwachung des öffentlichen Raumes der Wendeschleife relevant, da die Bewohner und Passanten auf die Nutzung des überwachten Bereichs angewiesen sind. Im Übrigen erzeugen Videokameras und Kameraattrappen den gleichen psychischen Überwachungsdruck auf die betroffenen Personen aus. Daher sind die Grundrechtsbeeinträchtigungen von echter Kamera und Attrappe identisch zu bewerten. Die schutzwürdigen Interessen der Betroffenen würden auch bei einer Kameraattrappe mögliche Interessen des Betreibers zur Wahrnehmung des Hausrechts überwiegen.

Der TLfDI erwägt, gegen den Betreiber eine Anordnung nach § 38 Abs. 5 BDSG zu erlassen. Daher hat der Betreiber der Videokamera eine letzte Frist zur Stellungnahme und Neuausrichtung bzw. Demontage der Kamera erhalten.

Wenn auch, entgegen den Angaben des Betreibers einer Kamera, Anhaltspunkte und Beweise gegeben sind, dass eine Videokamera betrieben wird, kann der TLfDI Maßnahmen ergreifen, um datenschutzkonforme Zustände wiederherzustellen. Diese kann er insbesondere mit dem Mittel der Anordnung nach § 38 Abs. 5 BDSG durchsetzen.

4.34 "Big Brother" unter Mietern – Videogaga 33

Wie bereits mehrfach in diesem Tätigkeitsbericht ausgeführt, werden vielerorts einfach Videoüberwachungsanlagen in Wohnanlagen installiert, ohne dass sich die verantwortliche Stelle Gedanken über die datenschutzrechtliche Zulässigkeit solcher Einrichtungen macht. Auch in diesem Fall hatte ein Bewohner sich über eine auf dem Balkon eines Nachbarn installierte Kamera beschwert.
Mit einem umfassenden Fragenkatalog und der Bitte um Stellungnahme zu der Videoüberwachungsanlage wandte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an den Nachbarn. Weiterhin wurde dieser vom TLfDI aufgefordert, Nachweise, wie zum Beispiel einen Lageplan des Hauses und vom Parkplatz, den Standort der Kamera und einen Screenshot, einzureichen.
Der Nachbar teilte daraufhin dem TLfDI in seiner ausführlichen Stellungnahme mit, dass er keinen öffentlich zugänglichen Bereich, hier den Parkplatz, videoüberwacht habe, denn die Videokamera sei nicht angeschlossen gewesen. Es habe sich lediglich um eine Attrappe gehandelt. Diese habe er zu seinem eigenen Schutz und zum Schutz seines PKW angebracht. Vor allem sei sein PKW in der Vergangenheit mehrfach beschädigt worden. Dies konnte der Nachbar dem TLfDI auch anhand von Tagebuchnummern belegen.
Wie in diesem Tätigkeitsbericht schon mehrfach durch den TLfDI verdeutlicht (s. Beitrag Nummer 4.27), unterscheiden sich solche Attrappen in ihrer datenschutzrechtlichen Prüfung kaum von richtigen Kameras. Dies liegt vor allem daran, dass es subjektiv für den Betroffenen keinerlei Unterschied macht, ob eine Kamera in Betrieb bzw. ausgeschaltet ist, oder ob es sich um eine Attrappe handelt. Denn der Zustand einer solchen Videoüberwachung ist von außen für die Betroffenen nicht erkennbar. Im Ergebnis bleibt daher der Überwachungsdruck für die Betroffenen gleich. Genau das führt zu

einer Verhaltensveränderung und stellt damit einen Eingriff in das allgemeine Persönlichkeitsrecht dar.
Daher sind Attrappen nur zulässig, wenn auch eine funktionstüchtige Kamera zulässig wäre. Dies bestimmt sich bei Außenkameras in der Regel und auch in diesem Fall nach § 6b Bundesdatenschutzgesetz (BDSG). Nach § 6b Abs. 1 BDSG ist eine Videoüberwachung nur zur Durchsetzung des Hausrechts oder zur Wahrnehmung berechtigter Interessen zu konkret festgelegten Zwecken zulässig, wenn sie hierfür erforderlich ist und keine Anhaltspunkte gegeben sind, dass schutzwürdige Interessen Betroffener überwiegen.
In diesem Fall konnte der Betreiber der Kamera darlegen, dass eine konkrete Gefährdungslage besteht. Dabei handelt es sich um berechtigte Interessen. Auch waren keine Anhaltspunkte ersichtlich, warum schutzwürdige Interessen Dritter überwiegen, da die Kameraattrappe erkennbar nur auf seinen PKW ausgerichtet war. Daher wurde diese im Ergebnis als zulässig bewertet.
Dennoch teilte der Betreiber mit, er habe die Attrappe abgebaut. Das Verfahren ist beendet.

Auch bei Kameraattrappen ist der Überwachungsdruck der gleiche wie bei einer funktionstüchtigen Kamera. Daher sind auch Attrappen nur zulässig, wenn eine funktionstüchtige Kamera zulässig wäre. Dies bestimmt sich bei Außenkameras in der Regel nach § 6b BDSG.

4.35 Wildkamera ohne Aufzeichnung – Videogaga 34

Immer wieder fühlen sich Nachbarn durch Videoüberwachung belästigt. In diesem Fall gab eine „Wildkamera“ Anlass zur Beschwerde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Kamera war an einem Fensterbrett des Wohnhauses des Nachbarn montiert. Die Beschwerdeführer fühlten sich in ihrem Persönlichkeitsrecht massiv gestört. In einem Schlichtungsverfahren vor dem zuständigen Gericht zwischen dem Nachbarn und dem Beschwerdeführer in einer anderen Angelegenheit des Nachbarschaftsstreites wurde die Kamera zwar thematisiert, aber nicht weiter bewertet. Vielmehr gab der Richter dem Beschwerdeführer den Tipp, sich an den TLfDI zu wenden.
Der Kamerabetreiber wurde mit einem umfangreichen Fragenkatalog zur Videoüberwachung konfrontiert. Die Antwort des Kamerabetrei-

bers ließ gar nicht lang auf sich warten. Es wurde mitgeteilt, dass die Kamera entfernt wurde. Die Kamera sei ohnehin eine Attrappe gewesen und habe keine Videoaufzeichnungen gespeichert. Selbst wenn die Kamera eine Attrappe war, wäre diese ebenso zu bewerten gewesen wie ein funktionstüchtiges Modell. Beide Varianten erzeugen denselben psychischen Überwachungsdruck, indem sie beim Betroffenen den Anschein erwecken, überwacht zu werden. Dies stellt auch bei einer Attrappe einen Eingriff in das Persönlichkeitsrecht dar. Von einer Videoüberwachung betroffene Personen ändern ihr Verhalten, wenn sie wissen oder glauben, dass sie überwacht werden.

Videokameras und auch Kameraattrappen erzeugen einen psychischen Überwachungsdruck und erwecken beim Betroffenen den Anschein, überwacht zu werden. Dies stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Von einer Videoüberwachung betroffene Personen ändern in den häufigsten Fällen ihr Verhalten, wenn sie wissen, dass sie überwacht werden.

4.36 Zulässigkeit von Kameraattrappen in der Nachbarschaft – Videogaga 35

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über zwei installierte Kameras des Nachbarn. Eine Kamera habe der Nachbar an der Hauswand, die andere an der Scheunenwand angebracht. Beide Kameras seien auf den öffentlichen Raum, sprich auf den Gehweg ausgerichtet gewesen. Auf Nachfrage bei dem Betreiber der Kameras, teilte dieser dem TLfDI mit, dass es sich bei den von ihm angebrachten Kameras lediglich um Attrappen und nicht um echte Kameras gehandelt habe. Der TLfDI informierte den Betreiber der Kameras darüber, dass Kameraattrappen datenschutzrechtlich genauso wie das funktionierende Modell zu behandeln seien. Mit dem Einsatz von Kameraattrappen ist ebenfalls ein Eingriff in das allgemeine Persönlichkeitsrecht verbunden, denn die Kameraattrappe soll bei den Betroffenen die Vorstellung einer funktionsfähigen Anlage erzeugen, um sie von einem unerwünschten Verhalten abzuhalten. Gerade von Kameraattrappen, die aus objektiver Sicht den Anschein der Echtheit erwecken, geht derselbe Anpassungs- und Überwachungsdruck wie von funktionstüchtigen Kame-

ras aus. Die Aufstellung einer solchen Attrappe stellt für den Betroffenen die dauernde Androhung einer Videoüberwachung dar. Die betroffene Person sieht sich damit in jedem Fall einer Kontrollmöglichkeit ausgesetzt. Die unbefangene, von Zwangswirkungen freie Kommunikation, Interaktion und Darstellung in der Öffentlichkeit ist aber Grundbedingung für die freie Entfaltung der Persönlichkeit.
Auch wurde bereits über die Zulässigkeit von Kameraattrappen vom TLfDI ausführlich im Tätigkeitsbeitrag Nummer 4.27 berichtet. Auf diesen wird hier Bezug genommen.
Letztendlich teilte aber der Betreiber dem TLfDI mit, dass er die Kameraattrappen entfernt habe. Dies bestätigten dem TLfDI auch die beschwerdeführenden Nachbarn. Damit konnte der TLfDI das Verfahren abschließen.

Aufgrund des auch von Attrappen ausgehenden Überwachungsdrucks auf Betroffene und deren mit richtigen Kameras identischer Außenwirkung behandelt der TLfDI diese nicht anders als funktionierende Kameras.

4.37 Neighbour is watching you – Videogaga 36

So heißt es überall dort, wo Videokameras zu Überwachungszwecken eingesetzt werden. Vor allem Nachbarn sehen sich unweigerlich der Überwachung durch andere Nachbarn ausgesetzt. Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen zum Einsatz von Videokameras zum Schutz des privaten Eigentums.
So auch im nachfolgenden Fall. Ein Bürger wandte sich an den TLfDI um sich über die Zulässigkeit einer von ihm auf seinem Grundstück geplanten Videoüberwachung mit vier Kameras beraten zu lassen. Als Grund für die geplante Videoüberwachung gab der Bürger, unter Vorlage entsprechender Tagebuchnummern der Polizei, zwei bereits stattgefundene Raubüberfälle auf seinem Grundstück an. Dem Bürger war es vor allem wichtig, auch Bereiche außerhalb seines Grundstücks aufzuzeichnen. Dadurch wollte er feststellen, ob sein Objekt von potentiellen Tätern ausgekundschaftet wird.
Der TLfDI stellte im Ergebnis fest, dass eine Videoüberwachung im vorliegenden Fall mit den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) vereinbar ist, allerdings nicht in dem vom Bürger gewünschten Umfang. Grundsätzlich findet das BDSG auf jeden

Umgang mit personenbezogenen Daten Anwendung. Gerade bei einer Videoüberwachung werden personenbezogene Daten erhoben und gegebenenfalls gespeichert.
Einziger Ausschlussgrund für nicht-öffentliche Stellen, wie auch in diesem Fall, stellen die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten für ausschließlich persönliche oder familiäre Tätigkeiten dar, § 1 Abs. 2 Nr. 3 2. Hs BDSG. Der Ausschlussgrund der persönlichen oder familiären Tätigkeit ist nur dann gegeben, wenn der Umgang mit den personenbezogenen Daten ausschließlich innerhalb der persönlichen oder familiären Sphäre (z. B. Grundstück, Familienangehörige) desjenigen vorgenommen wird, der die Daten verarbeitet (also erhebt, speichert, nutzt etc.). In einer am 11. Dezember 2014 ergangenen Entscheidung hat der Europäische Gerichtshof (EuGH, Urteil vom 11. Dezember 2014, C212/13) klargestellt, dass jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre des Betreibers gerichtet ist, unter den Anwendungsbereich der Europäischen Datenschutzrichtlinie und damit in den des BDSG fällt. (siehe dazu auch Anlage 19)**.** Eine Videoüberwachung ist damit nur unter den dort geregelten Voraussetzungen zulässig. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Der Aufnahmebereich der hier geplanten vier Kameras sollte zwar das Grundstück des Bürgers erfassen, darüber hinaus aber auch den Gehweg sowie Nachbargrundstücke. Daher kam der TLfDI zu dem Ergebnis, dass das BDSG im vorliegenden Fall anwendbar ist.
Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen und damit gefilmten Personen eingewilligt haben. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen.
Als mögliche gesetzliche Grundlage für die Zulässigkeit einer Videoüberwachung, welche die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt, kommt § 6b BDSG in Betracht. Bei öffentlich zugänglichen Räumen handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. Grundstücks-

eigentümers) von jedermann genutzt oder betreten werden dürfen. Nicht öffentlich zugänglich sind demgegenüber Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Die Einordnung als nicht öffentlich zugänglicher Raum hängt jedoch vom Einzelfall ab. Wie bereits ausgeführt, liegt eine Überwachung öffentlich zugänglicher Räume auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden.

Im vorliegenden Sachverhalt plante der anfragende Bürger, unter Vorlage entsprechender Bildausschnitte, eine Installation von vier Kameras mit Ausrichtung auf den an sein Grundstück angrenzenden Gehweg sowie auf Nachbargrundstücke, und damit auf den öffentlich zugänglichen Raum.

Nach § 6b BDSG ist die Beobachtung und Aufzeichnung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Hausrecht umfasst die Befugnis, grundsätzlich frei darüber zu entscheiden, wem der Zutritt zu einer Örtlichkeit gestattet und wem er verwehrt wird. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Dafür sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit, nachzuweisen.

Im Ergebnis geht jedoch der TLfDI bei einem Gehweg, der von einer Vielzahl von Personen genutzt werden kann, davon aus, dass die schutzwürdigen Interessen der Betroffenen, nicht gefilmt und aufgezeichnet zu werden, die Interessen des Bürgers und seiner Familie, eine Videoüberwachung durchzuführen, überwiegen.

Der TLfDI erteilte dem Bürger für seine geplante Videoüberwachung den Hinweis, die Nachbargrundstücke und den öffentlichen Gehweg entweder durch Neuausrichtung der Kameras oder durch Schwärzung der entsprechenden Bereiche von der Videoüberwachung auszunehmen.

Die Videoüberwachung des eigenen, allein genutzten, abgegrenzten Grundstücks unterfällt in der Regel nicht dem BDSG, vergleiche § 1 Abs. 2 Nr. 3 2. Hs. BDSG. Dies ändert sich für Bereiche, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen, so zum Beispiel der Weg zur Klingel oder zum Briefkasten. Hier ist das BDSG anwendbar. Nach § 6b BDSG ist die Beobachtung und Aufzeichnung solcher öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Anhaltspunkte überwiegen in der Regel dann, wenn die eigenen Grundstücksgrenzen überschritten werden.

4.38 Wohnanlage unter Beobachtung – Videogaga 37

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er teilte mit, dass er in einer Wohnanlage wohne, in der nach dem Einzug von Bürgerkriegsflüchtlingen in der Nachbarschaft eine flächendeckende Videoüberwachung im Außenbereich eingerichtet worden sei. Hinweise auf die Videoüberwachung fehlten. Er hielt die Maßnahmen für unrechtmäßig.
Auf die Anfrage des TLfDI gab das Unternehmen, das die Wohnanlage verwaltete, Auskunft: Es gab zwölf Videokameras, die den Außenbereich der Wohnanlage beobachteten und für 72 Stunden aufzeichneten. Zu jeder Kamera wurde ein Screenshot des Aufnahmebereichs mit eingereicht. Es war zu erkennen, dass die Bereiche geschwärzt waren, in denen die Kamera auf Balkone oder Fenster der Bewohner gerichtet war. Mehrere Bereiche der Anlage wurden von zwei Kameras aus leicht unterschiedlichen Blickwinkeln beobachtet. Aufgenommen wurden auch ein parkartiger Bereich mit einem kleinen Spielplatz sowie der zur Anlage gehörende Parkplatz. Auf den Aufnahmen waren die Nummernschilder der geparkten Autos gut zu erkennen. Hinweisschilder waren mittlerweile angebracht worden. Als Grund für die Videoüberwachung war angegeben worden, dass es immer wieder Vorfälle mit ruhestörendem Lärm, Vandalismus und Verunreinigungen gegeben habe.

Nach einer ersten Einschätzung des TLfDI ist die Videoüberwachung in dem betriebenen Umfang nicht zulässig. Dem Betreiber wurde mitgeteilt, dass nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig ist, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Um die Zulässigkeit der Videoüberwachung prüfen zu können, benötigt der TLfDI zu jeder einzelnen Kamera die Angabe des Zwecks der Videoüberwachung. Der Betreiber wurde darauf hingewiesen, dass zwar grundsätzlich ein berechtigtes Interesse darin zu sehen ist, wenn die Videoüberwachung dazu eingesetzt werden soll, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen. Dann muss aber eine tatsächliche Gefahrenlage nachgewiesen werden. Zu fordern ist die Dokumentation konkreter Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Es ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG. Es bedarf außerdem schriftlicher Festlegungen dazu, unter welchen Voraussetzungen durch wen Einsicht in die Aufnahmen genommen werden darf und auf welche Weise eine Protokollierung der Einsichtnahme sichergestellt ist. Zu den verfolgten präventiven Zwecken wurde der Betreiber darauf hingewiesen, dass eine reine Aufzeichnung für präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. Sicherheitspersonal unmittelbar eingreifen kann.
Der Betreiber wurde aufgefordert zu prüfen, ob die von ihm verfolgten Zwecke tatsächlich mit Videoüberwachung erreicht werden können. An der Erforderlichkeit der Videoüberwachung bestanden beispielsweise deswegen Zweifel, weil für den gleichen Aufnahmebereich mehrere Kameras in Betrieb sind. Außerdem bestanden nach Auffassung des TLfDI bei etlichen Aufnahmebereichen Anhaltspunkte dafür, dass schutzwürdige Interessen der Betroffenen überwiegen. Dies gilt insbesondere für den parkartigen Bereich, den Spielplatzbereich und den Parkplatz, weil sich dort eine Vielzahl von

Personen aufhalten können, die grundsätzlich Anspruch darauf haben, beispielsweise ihren Freizeitinteressen unbeobachtet nachgehen zu können.
Vor der Inbetriebnahme einer Videoüberwachung ist eine Vorabkontrolle nach § 4d Abs. 5 BDSG erforderlich, wenn bei dem Einsatz der Videotechnik von besonderen Risiken für die Rechte und Freiheiten der Betroffenen auszugehen ist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Hiervon ist bei der hier betriebenen Videoüberwachung auszugehen. Der betriebliche Datenschutzbeauftragte (bDSB) hat gemäß § 4d Abs. 6 BDSG die Vorabkontrolle durchzuführen und das Ergebnis sowie die Begründung schriftlich zu dokumentieren. Sollte es bei dieser Anzahl der zum Einsatz kommenden Videokameras bleiben, ist auf jeden Fall ein Datenschutzbeauftragter zu bestellen und eine Vorabkontrolle vorzunehmen.
Der Betreiber wurde aufgefordert zu prüfen, welche Kameras er unter Berücksichtigung der Hinweise des TLfDI zukünftig weiter betreiben will. Für diese Kameras muss er den konkreten Zweck benennen und ggf. Nachweise für eine tatsächliche Gefahrenlage erbringen. Erst danach ist eine abschließende Bewertung des Vorgangs möglich.

Vom Betreiber einer Videoüberwachung ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Weiterhin muss er prüfen, ob die von ihm verfolgten Zwecke tatsächlich mit der Videoüberwachung erreicht werden können. Der Überwachungszweck jeder einzelnen Kamera ist gesondert und konkret schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG.

4.39 Amtshilfeersuchen – Videogaga 38 – Ordnungsamt kontrolliert vor Ort

Eine Familie hatte diverse Antennen auf dem Dach des Nachbarn entdeckt. Weiterhin wurde eine Kamera am oberen Fenster des Hauses festgestellt. Diese war genau auf die Grundstücke der Familie gerichtet. Die Familie sprach den Nachbarn auf ihre Feststellungen an und bat ihn, die Antennen und die Kamera zu entfernen. Darauf reagierte der Nachbar nicht. Die Familie wandte sich deshalb an den

Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Betreiber der Kamera wurde mit einem ausführlichen Fragebogen mit einem Auskunftsverlangen des TLfDI kontaktiert. Der TLfDI erhielt in der Folge einen anonymen Brief, in dem mitgeteilt wurde, dass es sich um eine Verwechselung handele. Es wurde weiter ausgeführt, dass an der besagten Adresse keine Videoüberwachung betrieben werde. War das ein Versuch, den TLfDI ruhig zu stellen?
Das Ordnungsamt der Stadt nahm nach einem Amtshilfeersuchen des TLfDI eine Vorortkontrolle vor und konnte insgesamt drei Kameras feststellen. Die von der Familie gemeldeten Antennen befanden sich auf dem Dach des Wohnhauses. Dem TLfDI wurde seitens der Stadt ein ausführlicher Kontrollbericht einschließlich Bildmaterial übersandt. Der TLfDI wird die angebrachte Videoüberwachungsanlage prüfen und, wenn notwendig, die Neuausrichtung oder Deinstallation der Kameras gemäß § 38 Abs. 5 Bundesdatenschutzgesetz (BDSG) anordnen.
Gegebenenfalls wird ein Bußgeldverfahren eingeleitet werden.

Über ein Amtshilfeersuchen kann der TLfDI auch Vorortkontrollen vom zuständigen Ordnungsamt durchführen lassen. Auf Grundlage der Zuarbeit des Ordnungsamtes wird die Videoüberwachungstechnik einer umfangreichen Prüfung unterzogen. Soweit es notwendig ist, ordnet der TLfDI die Neuausrichtung oder Deinstallation der Kameras gemäß § 38 Abs. 5 BDSG an. Es kann sich auch ein Bußgeldverfahren anschließen.

4.40 Achtung Kamera! Die private Videoüberwachung – Videogaga 39

Im Berichtszeitraum meldete sich ein besorgter Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er gab an, dass die Eigentümer eines Objekts eine Videokamera installiert hätten. Außerdem sei die Videokamera auf den vor dem Haus verlaufenden Gehweg ausgerichtet gewesen. Nachdem der TLfDI das Grundbuchamt im Rahmen der Amtshilfe nach § 24 Abs. 1 Satz 1 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) um Auskunft bezüglich des Eigentümers des Hauses gebeten hatte, konnte ein Thüringer Unternehmen als Eigentümerin festgestellt werden. Das Unternehmen teilte dem TLfDI mit, dass das

Objekt an eine Privatperson veräußert worden sei. Diese Privatperson forderte der TLfDI auf, zu der Videoüberwachung Stellung zu nehmen.
Auf diese Anfrage hin wurde dem TLfDI mitgeteilt, dass insgesamt drei Kameras an dem Objekt angebracht waren. Der Betreiber hatte die Kameras nach mehrfachen Beschädigungen am Haus zur Überwachung des Innenhofes und zum Schutz der Mieter installiert. Dieser Innenhof war geschlossen und lediglich für die Betreiber zugänglich, nicht aber für die Öffentlichkeit. Weiterhin lief das Kamerasystem über eine Live-Übertragung (Eins-zu-Eins-Übertragung) ohne Aufzeichnungsmöglichkeit.
Im Ergebnis stellte der TLfDI fest, dass die Videoaufnahmen nur den privaten Bereich betrafen und zu ausschließlich privaten Zwecken erfolgten, weswegen eine Zuständigkeit des TLfDI nicht gegeben war, vergleiche § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG). Hintergrund war das am 11. Dezember 2014 ergangene Urteil des Europäischen Gerichtshofs (EuGH). Dort hat der EuGH im Rahmen eines Vorabentscheidungsverfahrens über die Auslegung von Art. 3 Abs. 2 der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bestätigt, dass auf eine privat betriebene Videoüberwachungsanlage unter bestimmten Voraussetzungen die Europäische Datenschutzrichtlinie und damit das insoweit gleichlautende Bundesdatenschutzgesetz anwendbar ist. Der EuGH stellte klar, dass jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa weil sie öffentlich zugänglichen Raum erfasst, in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes (BDSG) falle; sie ist damit nur unter den dort geregelten Voraussetzungen zulässig. Hier handelte es sich um einen geschlossenen Innenhof und damit um einen nicht öffentlich zugänglichen Raum, der nur den Betreibern und damit einem bestimmten und abschließend definierten Personenkreis zugänglich war. Daher findet das BDSG hier keine Anwendung, was wiederum die Zuständigkeit des TLfDI ausschloss. Das Verfahren konnte mangels Zuständigkeit des TLfDI abgeschlossen werden.

Nach dem Urteil des EuGH fällt jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie öffentlich zu-

gänglichen Raum erfasst, in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes (BDSG).

4.41 Garten außer Rand und Band – Videogaga 40 – Videoüberwachung durch Nachbarn

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Sommer 2015 im Rahmen einer Nachbarschaftsstreitigkeit die typischen datenschutzrechtlichen Probleme in diesen Fällen zu bewerten. Videokameras! Wie so oft setzte eine Videoüberwachung das i-Tüpfelchen im Streit zwischen zwei Nachbarn. In diesem Fall war es eine besondere Konstellation, da die Nachbarn Geschwister waren. Sie hatten jedoch keinen persönlichen Kontakt zueinander. Die Schwester zeigte dem TLfDI die Videoüberwachung im Garten des Bruders an. Bei einer angekündigten Vorortkontrolle, die im Einverständnis mit dem Bruder stattfand, stellte der TLfDI insgesamt drei Kameras fest. Eine Kamera befand sich auf einem Brett, montiert an einem Komposthaufen, und die anderen beiden Kameras wurden mit einer grünen Abfalltonne getarnt. Aber damit noch nicht genug. Die Terrasse und das Wohnzimmerfenster der Schwester lagen im Aufnahmebereich einer der Kameras. Eine weitere Kamera hatte den Blickwinkel in Richtung der Terrasse der Schwester ausgerichtet. Diese beiden Kameras waren mit einer aufwändigen Verkabelung versehen. Diese führte über einen Kabelkanal in den Schuppen des Bruders. Im Schuppen endete die Verkabelung. Ein Aufnahmegerät war nicht (mehr) angeschlossen.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen, Privatpersonen) wird durch das Bundesdatenschutzgesetz (BDSG) geregelt, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben, § 1 Abs. 2 BDSG. Der TLfDI hat hingegen keine Zuständigkeit inne, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 (C 212/13) ist diese Regelung allerdings eng auszulegen. Wie in Anlage 19 bekannt gegeben, ist entscheidend, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären

Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen videoüberwacht werden, die mit dem Videobetreiber nicht in einer persönlichen Nähebeziehung stehen. Der Aufnahmebereich der hier kontrollierten Kameras erfasste zwar das Grundstück der Schwester, jedoch kam der TLfDI zu dem Ergebnis, dass das BDSG im vorliegenden Fall anwendbar ist. Insbesondere deshalb, weil zwischen den Geschwistern kein familiäres Verhältnis gepflegt wurde und es damit an der notwendigen Nähebeziehung für den Ausschluss des BDSG fehlte.

Zwei der drei Kameras wurden durch den TLfDI als unzulässig bewertet. Die Videoüberwachung dieser Kameras scheiterte bereits an der Erforderlichkeit, da die Videoüberwachung über die Grundstücksgrenzen des Bruders hinausging. Denn nur die zur Zweckerreichung notwendigen Bereiche dürfen im Blickwinkel der Kamera liegen. Dazu gehört nicht das Grundstück der Schwester. Außerdem stellten die Kameras einen erheblichen Eingriff in das Persönlichkeitsrecht der Schwester dar. Ihre Terrasse und ihr Wohnzimmerfenster sowie Teile des Grundstücks lagen im Fokus der Kameras. Dadurch hätten höchstpersönliche Lebensbereiche der Schwester eingesehen werden können. Eine Kamera erzeugt einen starken psychischen Überwachungsdruck. Dies gilt umso mehr, als die Schwester diesem Überwachungsdruck rund um die Uhr ausgesetzt war. Sie konnte sich der Videoüberwachung des Bruders nur entziehen, indem sie ihre Terrasse mied und das Rollo vom Wohnzimmerfenster geschlossen hielt. Eine freie Entfaltung der Persönlichkeit, welche im Grundgesetz in Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 Grundgesetz jedem zugesprochen wird, war somit nicht möglich. Aus diesem Grund hat es auf die Anwendbarkeit des BDSG auch keinen Einfluss, dass die Kameras zum Zeitpunkt der Kontrolle keine Aufnahmen aufzeichneten. Eine Kameraattrappe erzeugt den gleichen psychischen Überwachungsdruck auf die betroffene Person wie eine funktionstüchtige Kamera, sodass die Grundrechtsbeeinträchtigung von echter Kamera und Attrappe identisch ist. Im vorliegenden Fall überwogen die schutzwürdigen Interessen der Schwester an deren Recht auf informationelle Selbstbestimmung die Interessen zur Abwehr von verbalen Angriffen der Schwester gegenüber des Kamerabetreibers.

Gegen den Bruder wird gemäß § 38 Abs. 5 BDSG eine Anordnung zum Abbau der beiden strittigen Kameras erlassen werden.

In Ausnahmefällen ist das BDSG auch anwendbar, wenn Familienmitglieder in den Erfassungsbereich der Kamera gelangen. Nach dem EUGH-Urteil vom 11. Dezember 2014 (C 212/13) kommt es darauf an, ob die erfassten Personen in einer persönlichen Nähebeziehung zum Betreiber stehen. Im Übrigen erzeugen Kameraattrappen den gleichen psychischen Überwachungsdruck wie eine angeschlossene Kamera. Der TLfDI ist daher der Auffassung, dass auch Kameraattrappen wie tatsächlich angeschlossene Kameras zu bewerten sind.

4.42 Wer hat mich angeschwärzt? – Videogaga 41

Auf einen Hinweis hin wurde der Thüringer Landebeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wieder einmal wegen einer Videokamera tätig, die ein Hausbesitzer an seiner Eingangstür angebracht hatte. Ausgerichtet war sie auf ein anderes Privatgrundstück. Der TLfDI schrieb den Betreiber der Videokamera mit der Bitte um Stellungnahme zur Angelegenheit an. Der erstaunte und verärgerte Betreiber führte aus, dass er weder an der Haustür noch sonst irgendwo an dem Haus oder auf dem Grundstück eine Videokamera installiert habe. Er forderte den TLfDI auf, seinen Informanten zu benennen, um ihn anzeigen zu können. Dieser Forderung konnte der TLfDI nicht nachkommen. Grundsätzlich darf sich jedermann an den TLfDI wenden, der meint, in seinem Recht auf informationelle Selbstbestimmung verletzt zu sein, § 11 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Aus dieser Anrufung des TLfDI darf aber kein Nachteil für den Beschwerdeführer entstehen, weil er von seinem vorgenannten Recht nach Abs. 1 Gebrauch macht, vergleiche § 11 Abs. 2 ThürDSG. Dazu verwies der TLfDI auf das Urteil des Verwaltungsgerichts Bremen vom 30. März 2010 (Az.: 2 K 548/09). Die dort herangezogene Norm findet ihre Entsprechung in § 13 ThürDSG. Das VG Bremen entschied, dass die Aufsichtsbehörde grundsätzlich gehalten ist, von dem Petenten gemachte Angaben vertraulich zu behandeln und damit auch seinen Namen nicht preiszugeben. Dazu bedarf es ganz besonderer Umstände, um dagegen berechtigte Interessen ins Feld zu führen.
Aber selbst im Falle eines Antrages auf Akteneinsicht würden Hinweise auf den Anzeigeerstatter in den meisten Fällen geschwärzt werden. Denn die Behörde hat nach § 29 Abs. 1 Thüringer Verwal-

tungsgesetz (ThürVwVfG) den Beteiligten eines Verfahrens die Einsicht in die betreffenden Akten nur insoweit zu gestatten, als deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Für eine Anzeige bedarf es aber nicht des Namens des Informanten. Vielmehr kann auch eine Anzeige gegen Unbekannt erstattet werden. Für die Ermittlung des Namens ist die Staatsanwaltschaft zuständig.

Grundsätzlich darf sich jedermann an den TLfDI wenden, der meint, in seinem Recht auf informationelle Selbstbestimmung verletzt zu sein, § 11 Abs. 1 ThürDSG. Aus dieser Anrufung des TLfDI darf aber kein Nachteil für den Beschwerdeführer entstehen. Das Recht auf Akteneinsicht der Beteiligten in die Verwaltungsakte ergibt sich aus § 29 Abs. 1 ThürVwVfG. Danach kann die Behörde den Beteiligten eines Verfahrens die Einsicht in die betreffenden Akten gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Die Namen eventueller Informanten sind hierfür in der Regel nicht erforderlich und daher regelmäßig zu schwärzen.

4.43 Domekamera in der Nachbarschaft – Videogaga 42

Aufgrund eines Hinweises erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, dass ein Nachbar an seinem Haus eine Domekamera angebracht hatte. Eine Domekamera ist eine Überwachungskamera, die unter einer halbrunden getönten Kuppel aus Kunststoff eingebaut ist, weswegen die Kamera und ihre Aufnahmerichtung von außen nicht zu erkennen sind. Rechts und links neben dem Gebäude verlief eine öffentliche Straße. Daraufhin forderte der TLfDI den Betreiber der Videokamera auf, einen umfangreichen Fragenkatalog, unter anderem zum Zweck der Kontrolle, zu beantworten und die angeforderten Nachweise, wie zum Beispiel den Standort der Kamera und Screenshots, beim TLfDI einzureichen. Der Betreiber antwortete dem TLfDI, dass er die angebaute Videokamera an dem zum damaligen Zeitpunkt im Umbau befindlichen und somit leerstehenden Haus zur Überwachung der Eingangstür eingesetzt habe. Diese sei aufgrund des Leerstandes des Hauses die größte Schwachstelle gewesen. Da die Installation der Kamera nicht leicht gewesen sei, habe er die Kamera nicht in Betrieb genommen. Auch sei ihm die Abschreckung

wichtiger gewesen. Hinweisschilder auf die Videoüberwachung waren nicht vorhanden.
Der TLfDI teilte dem Betreiber der nicht funktionierenden Kamera mit, dass auch eine nicht funktionstüchtige Kamera oder eine Kameraattrappe ein erhebliches datenschutzrechtliches Problem darstellt, da Nachbarn, Passanten und sonstige Verkehrsteilnehmer nicht wissen können, dass hinter der Kamera kein Beobachtungs- bzw. Aufzeichnungssystem steckt. Daher entwickelt eine Kameraattrappe oder eine nichtfunktionstüchtige Kamera den gleichen Überwachungsdruck wie ein funktionierendes Modell, da gerade eine Videobeobachtung suggeriert werden soll. Wegen dieses gleichen Beobachtungsdrucks sind Attrappen daher nur unter denselben Bedingungen zulässig, die auch eine echte Kamera erfüllen muss. Dazu wird auf den Beitrag Nr. 4.27 in diesem Tätigkeitsbericht verwiesen.
Der TLfDI forderte den Betreiber der nicht funktionstüchtigen Kamera auf, die Kamera unverzüglich wegen des Verstoßes gegen § 4 Abs. 1 Bundesdatenschutzgesetz abzubauen.
Der einsichtige Betreiber entfernte die nicht funktionstüchtige Kamera. Das Verfahren war damit abgeschlossen.

Kameraattrappen haben dieselben Voraussetzungen zu erfüllen wie funktionsfähige Kameras, da sie denselben Überwachungsdruck beim Betroffenen auslösen.

4.44 Zuständig oder unzuständig, das ist hier die Frage – Videogaga 43

Wie so oft beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einer Beschwerde über den Einsatz von Überwachungskameras in der Nachbarschaft.
Der TLfDI konnte bisher zur Eröffnung des Anwendungsbereiches des BDSG keine abschließende Bewertung vornehmen. Grundsätzlich findet das BDSG auf jeden Umgang nicht-öffentlicher Stellen – wozu auch natürliche Personen zählen – mit personenbezogenen Daten Anwendung. Einziger Ausschlussgrund für nicht-öffentliche Stellen ist die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten für ausschließlich persönliche oder familiäre Tätigkeiten. Der Ausschlussgrund der persönlichen oder familiären Tätigkeit ist nur dann gegeben, wenn der Umgang mit den personen-

bezogenen Daten ausschließlich innerhalb der persönlichen oder familiären Sphäre desjenigen vorgenommen wird, der die Daten verarbeitet (also erhebt, speichert, nutzt, etc.). So hat es der Europäische Gerichtshof (EuGH, Urteil vom 11. Dezember 2014, C212/13) festgestellt. Dies ist jedenfalls dann nicht der Fall, wenn auch öffentlich zugängliche Bereiche von der Videoüberwachung miterfasst werden. Tatsächlich wird die persönliche oder familiäre Sphäre aber ebenfalls verlassen, wenn ein Teil eines fremden Grundstücks miterfasst wird.

Diese Konstellation kann vorliegend nicht ausgeschlossen werden. Nach derzeitigem Sachstand gibt es widersprüchliche Aussagen zum Erfassungsbereich der Kamera. Einerseits gibt es ein Gutachten, aus dem sich ergibt, dass die Kamera mit der derzeitigen Ausrichtung am Bildrand auch die Grundstücksgrenze der Beschwerdeführer aufzeichnet. Andererseits existiert ein zivilrechtliches Urteil, in dem das Gegenteil festgestellt wird.

Wenn das Kamerabild keinen öffentlich zugänglichen Raum erfasst und auch sonst die Kamera zu rein persönlichen Zwecken betrieben wird, würde dies zur Nichtanwendbarkeit des BDSG führen. Dies hätte zur Folge, dass der TLfDI für die Prüfung der betreffenden Kamera nicht zuständig wäre. Andernfalls würde eine Zuständigkeit bestehen und der TLfDI könnte die Vereinbarkeit der Datenverarbeitung durch die Kamera an den Maßstäben des BDSG messen. Sollte diese nicht den im BDSG festgeschriebenen Voraussetzungen entsprechen, könnten letztlich auch Anordnungen erlassen werden.

Um seine (Un-)Zuständigkeit festzustellen, stehen dem TLfDI grundsätzlich die in § 38 Abs. 3 und 4 BDSG genannten Instrumentarien zur Verfügung. Er kann also Auskünfte verlangen und Geschäftsräume sowie dazugehörige Grundstücke kontrollieren. Stellt er seine Unzuständigkeit fest, sind diese Aktivitäten jedoch sofort einzustellen.

Vorliegend herrscht auf Betreiberseite die Ansicht, der TLfDI wäre unzuständig, ohne jedoch hierzu irgendeine stichhaltige Begründung aufzuführen. Das kann in diesem Fall tatsächlich nicht ausgeschlossen werden. Um dies jedoch festzustellen, müssten die hierzu verlangten Auskünfte an den TLfDI erteilt werden. Derzeit weigert sich der Kamerabetreiber, dem nachzukommen. Der TLfDI wird diesem gegenüber die Sach- und Rechtslage nochmals ausführlich darlegen und erklären, wofür die verlangten Auskünfte notwendig sind. Sollte das nicht zum Erfolg führen wird der TLfDI gezwungen sein, ein

Ordnungswidrigkeitenverfahren wegen Nichterteilung von Auskünften einzuleiten.

Das BDSG findet grundsätzlich auf jeden Umgang nicht-öffentlicher Stellen – wozu auch natürliche Personen zählen – mit personenbezogenen Daten Anwendung, § 1 Abs. 1 BDSG. Einziger Ausschlussgrund für nicht-öffentliche Stellen sind die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten für ausschließlich persönliche oder familiäre Tätigkeiten, § 1 Abs. 2 Nr. 3, 2. Hs. BDSG. Videoüberwachung, die auf einen Bereich außerhalb der privaten Sphäre gerichtet ist, wird nicht von diesem Ausschlussgrund erfasst. Sie unterfällt den Regelungen des BDSG und ist nach § 6b BDSG zu beurteilen – so der EuGH.

4.45 Vorsicht Kameraattrappe! – Videogaga 44

Erneut erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Bürgers über eine installierte Videokamera an der Toreinfahrt eines Grundstücks. Die Videokamera sei so ausgerichtet, dass sie den öffentlichen Weg davor und auch das private Grundstück gegenüber überwache. Damit der TLfDI eine Bewertung der rechtlichen Zulässigkeit der betriebenen Videokamera vornehmen konnte, schrieb er den Betreiber der Videokamera mit der Bitte um Auskunft im Sinne des § 38 Abs. 3 Bundesdatenschutz (BDSG) an. Daraufhin teilte der Betreiber der Videokamera dem TLfDI mit, dass es sich bei der Videokamera lediglich um eine Attrappe handele, die nicht funktionstüchtig sei. Diese habe er aufgrund der vermehrten Einbrüche in seiner Region und der Waldnähe seines Grundstücks am Ortsrand angebracht. Die Attrappe sollte der Abschreckung möglicher Diebesbanden dienen.
Der Betreiber wurde vom TLfDI darauf hingewiesen, dass eine für echt gehaltene Attrappe von den betroffenen Bürgern ebenso als Grundrechtseingriff empfunden wird wie eine tatsächlich funktionierende Kamera. Dies hat der TLfDI bereits ausführlich in seinem Beitrag Nr. 4.27 in diesem Tätigkeitsbericht aufgeführt.
Vorliegend zeigte sich der Bürger einsichtig und entfernte die Kameraattrappe. Das Verfahren konnte vom TLfDI abgeschlossen werden.

Von Kameraattrappen geht der gleiche Überwachungsdruck wie von einer funktionstüchtigen Kamera aus.

4.46 Home sweet home – kein Videogaga 45

Ende März 2015 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Information, dass die Grundstücksbesitzer einen ehemaligen Bahnhof, gelegen im Thüringer Wald, erworben und dort eine Videoüberwachungsanlage installiert hatten. Der ehemalige Bahnhof war bereits im Jahr 1997 stillgelegt worden. Die Grundstückerwerber bauten das alte Bahnhofsgebäude nun zu einem Wohnhaus um. Personen, die das abgelegene und an einen Wald angrenzende Grundstück passierten, fühlten sich durch die Videoüberwachungsanlage beobachtet und befürchteten eine Verletzung ihrer Persönlichkeitsrechte. Insbesondere bezüglich des Zugangs zum benachbarten Grundstück der Deutschen Regionaleisenbahn bestand Unsicherheit über ein eventuelles Wegerecht zu Lasten des ehemaligen Bahnhofsgrundstückes. Der TLfDI führte eine Vorortkontrolle zur Sachverhaltsaufklärung mit dem Einverständnis des Grundstückseigentümers durch. Im Verlauf des Besichtigungstermins wurden insgesamt vier Kameras festgestellt, die nach Auskunft der Grundstückerwerber im Februar 2015 in Betrieb genommen worden waren. Seit Anfang des Jahres 2015 wurden auf dem Grundstück zwei Diebstähle und ein Unfall mit Fahrerflucht begangen und durch die Eigentümer zur Anzeige gebracht. Sämtliche Kameras wurden zum Schutz vor weiteren Straftaten und zur Beweissicherung für künftige Strafanzeigen und deren zivilrechtliche Verfolgung angebracht. Die Kameras überwachten ausschließlich das eigene Grundstück der Eigentümer. Auch die angrenzenden, noch bestehenden Bahnschienen wurden nicht videoüberwacht. Das Grundstück wies eine verwinkelte Bauweise der aneinandergrenzenden Gebäude auf.
Nach eingehender Prüfung konnte festgestellt werden, dass ein öffentliches Wegerecht auf dem Grundstück nicht bestand. Dazu legten die Eigentümer den Grundbuchauszug und den Kaufvertrag über das Grundstück vor. Das Bahnhofsgrundstück wurde weiterhin als Garten genutzt und sollte schnellstmöglich umzäunt werden. Die Eigentümer hatten einen entsprechenden Bauantrag bereits gestellt und erwarteten nunmehr lediglich die Erteilung der Baugenehmigung.

Bis dahin war das Grundstück nicht gegen den Zutritt Unbefugter gesichert.
Die Videoüberwachungsanlage der Familie wurde zunächst nach den Regelungen des § 6b Bundesdatenschutzgesetz (BDSG) bewertet. Demnach war eine Videoüberwachung von öffentlich zugänglichen Räumen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich war und keine Anhaltspunkte bestanden, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstanden. Eine Videoüberwachung zur Wahrnehmung des Hausrechts konnte neben der Beobachtung zu präventiven Zwecken auch als repressives Mittel zur Beweissicherung eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung zivilrechtlicher Schadensersatzansprüche zu ermöglichen (Scholz in Simitis, BDSG, 8. Auflage, § 6b, Rn. 75). Die Eigentumsverhältnisse am Beobachtungsobjekt waren für die Erfüllung des Tatbestandsmerkmals „öffentlich zugänglicher Raum“ allerdings unbeachtlich. Nicht öffentlich zugänglich sind hingegen Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Allein die faktische Zugangsmöglichkeit (hier: noch nicht vorhandener Gartenzaun) begründete keine Öffentlichkeit, da der entgegenstehende Wille aus den Umständen für die betroffenen Personen erkennbar war (Scholz in Simitis, BDSG, 8. Auflage, § 6b, Rn. 42, 43, 48). An dem Grundstück war deutlich sichtbar ein Hinweisschild angebracht, auf dem zum Ausdruck kam, dass Unbefugten das Betreten und Befahren des Grundstücks verboten war. Daher war § 6b BDSG hier nicht einschlägig.
Die Videoüberwachung konnte nach § 28 Abs. 1 Nr. 2 BDSG ebenfalls zulässig sein, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich war und kein Grund zu der Annahme bestand, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung und Nutzung überwog. Da die Familie über den Zweck und die Mittel der Überwachungstechnik und somit über die Verarbeitung von personenbezogenen Daten entschied, war sie die verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG (Dammann in Simitis, BDSG, 8. Auflage, § 3, Rn. 224). Die von ihr angebrachte Videoüberwachung diente zur Wahrnehmung des Hausrechts als repressives Mittel, und zwar zur Aufklärung von Straftaten

und der Verfolgung der sich daraus ergebenden zivilrechtlichen Ansprüche. Um darin grundsätzlich ein berechtigtes Interesse zu sehen, musste eine tatsächliche Gefahrenlage nachgewiesen werden. Aufgrund der bisher auf dem Grundstück verübten Vermögensdelikte war eine tatsächliche Gefahrenlage hinreichend belegt. Auch war in diesem Fall die Erforderlichkeit der Videoüberwachung gegeben, da die Eigentümer die Aufnahmen nur aufzeichneten, wenn sie selbst nicht auf dem Grundstück anwesend waren. Eine mögliche Alternative zur Videoüberwachung wären regelmäßige Kontrollgänge von Bewachungspersonal gewesen. Dies wäre für die Familie wiederum ein enormer finanzieller Aufwand gewesen, der außer Verhältnis zum verfolgten Zweck gestanden hätte. Eine zusätzliche Absicherung des Grundstücks hätte der Gartenzaun dargestellt. Auf den Zeitpunkt für dessen Genehmigung hatten die Eigentümer seit der Beantragung der Baugenehmigung keinen Einfluss mehr. Zur Aufklärung von Straftaten, insbesondere um den Täter aufzudecken, gab es daher im vorliegenden Fall kein milderes und für die Betroffenen weniger einschneidendes Mittel.
Die schutzwürdigen Interessen der Betroffenen wurden umfangreich geprüft. Da die montierten Kameras ausschließlich das eigene Grundstück überwachten, konnten Fußgänger, die das Grundstück lediglich passierten, aber nicht betraten, nicht in den Aufnahmebereich der Kameras geraten. Der zunächst mit einem öffentlichen Wegerecht vermutete Weg gehörte teilweise zum Grundstück der Erwerber. Der andere Teil, einschließlich der Bahngleise, gehörte der Deutschen Regionaleisenbahn. Diese war auch für die Pflege des Grundstücks und der Bahnstrecke zuständig. Um Pflegearbeiten an der Bahnstrecke vorzunehmen, mussten die Mitarbeiter der Deutschen Regionaleisenbahn das Grundstück der Erwerber allerdings nicht betreten. Eine Auffahrt, die an das Grundstück der Familie angrenzt, ermöglichte die Zufahrt zum Grundstück der Deutschen Regionaleisenbahn. Von dort aus konnten die Mitarbeiter die Bahnstrecke und das dazugehörige Grundstück betreten. Hinweisschilder zur Videoüberwachung des eigenen Grundstücks waren eindeutig sichtbar angebracht. Es wurde darauf aufmerksam gemacht, dass es sich um ein Privatgrundstück handelt, dessen Betreten nicht erwünscht war. Somit konnten Betroffene nur widerrechtlich oder bewusst in den Aufnahmebereich geraten.
Im Ergebnis war die Nutzung der installierten Videoüberwachungsanlage nach den Bestimmungen des BDSG zulässig.

Ob und auf welcher Rechtsgrundlage eine Videoüberwachung zulässig ist, bedarf immer einer umfangreichen Einzelfallprüfung. Nicht öffentlich zugänglich sind Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Allein die faktische Zugangsmöglichkeit begründete keine Öffentlichkeit, wenn der entgegenstehende Wille aus den Umständen für die betroffenen Personen erkennbar ist.

4.47 Oh Tannenbaum – Videogaga 46 – Videoüberwachung des Gartens oder des öffentlich zugänglichen Bereichs?

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Beschwerde über den Inhaber einer Pension ein, der seinen Garten und auch einen Teil des öffentlichen Bereichs der Straße überwachen würde. Auf Anfrage des TLfDI teilte der Pensionswirt mit, dass sich auf seinem Grundstück vier Kameras befänden, die zum Schutz seines Privateigentums vor Vandalismus dienten. Auf dem Grundstück befände sich eine hohe Tanne, an der viele Lichterketten angebracht wären. Diese seien in der Vergangenheit wiederholt von Unbekannten durchgeschnitten worden. Weil es immer sehr aufwendig sei, die Lichterketten jährlich neu anzubringen, werden sie nicht abgenommen. Die vier Kameras seien nur auf die Tanne und nicht in den öffentlichen Bereich gerichtet. Um diese Behauptung zu verifizieren, forderte der TLfDI den Betreiber auf, Screenshots des jeweiligen Aufnahmebereichs der Kameras zu übersenden. Wie sich zeigte, war auf den Bildern von zwei Kameras tatsächlich nur die Tanne zu sehen. Diese Kameras zeichneten Personen einstellungsbedingt nur dann auf, wenn sie sich unmittelbar an der Tanne befanden. Eine weitere Kamera, die sich auf dem Erdboden befand, filmte hingegen schräg nach oben über den Gartenzaun und erfasst auch den Gehweg und das Nachbarhaus. Auf dem Bild zur letzten Kamera waren die Straße, der Gehweg beider Straßenseiten und der Gartenweg erkennbar. In den Aufnahmebereich dieser Kamera gelangten die Passanten der Gehwege beider Straßenseiten und Fahrzeuge. Zudem wurden alle Personen videografiert, die den Gehweg zum Eingang des Gebäudes benutzten. Einen Hinweis auf die Videoüberwachung gab es nicht.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist eine Videoüberwachung grundsätzlich wie jeder Umgang mit personenbezoge-

nen Daten nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung durch eine gesetzliche Vorschrift erlaubt wird. Eine Einwilligung kommt der Natur der Sache nach nicht in Betracht. Als Erlaubnisnorm kommt nur der § 6b BDSG in Frage, nach dem eine Videoüberwachung in einem öffentlich zugänglichen Raum zulässig ist, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Eine Videoüberwachung zur Wahrnehmung des Hausrechts kann neben der Beobachtung zu präventiven Zwecken auch als repressives Mittel zur Beweissicherung eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung zivilrechtlicher Schadensersatzansprüche zu ermöglichen. Diese Voraussetzungen waren aufgrund der vorangegangenen Beschädigungen gegeben.
Selbst wenn eine Videoüberwachung erforderlich ist, kann sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Hiervon kann nicht ausgegangen werden, wenn die aufgenommenen Bilder Personen nur erfassen, wenn sie unmittelbar an der Tanne stehen. Die schutzwürdigen Interessen der videoüberwachten Personen sind anders zu bewerten, wenn eine Kamera permanent und lückenlos Personen überwacht, die den Gehweg vor dem Grundstück, die öffentliche Straße oder den Gartenweg passieren, der zur Pension führt. Diese Personen haben keinen Anlass für ihre Überwachung gegeben. Es können Verhaltensmuster der Betroffenen erstellt werden. Die schutzwürdigen Interessen der videoüberwachten Personen überwiegen in Bezug auf diese Kameras die Interessen zur Wahrnehmung des Hausrechts. Anders zu beurteilen wäre dies, wenn der Aufnahmewinkel dahingehend geändert wird, dass die Kamera nur noch auf die Edeltanne gerichtet ist.
Der TLfDI beabsichtigt daher, gegenüber dem Inhaber der Pension nach § 38 Abs. 5 Satz 1 BDSG anzuordnen, einen Hinweis auf die Videoüberwachung nach § 6b Abs. 2 BDSG anzubringen und die Einstellung der Blickwinkel der Kameras so zu verändern, dass sich Bereiche außerhalb des Grundstückes nicht mehr auf den Aufnahmen befinden. Vor Erlass eines kostenpflichtigen Verwaltungsaktes wurde dem Pensionsinhaber nach § 28 Thüringer Verwaltungsver-

fahrensgesetz Gelegenheit zur Stellungnahme gegeben. Damit wird ihm auch die Gelegenheit gegeben, den Forderungen des TLfDI vor Erlass eines Bescheids nachzukommen.

Selbst wenn eine Videoüberwachung erforderlich ist, kann sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Hiervon ist in aller Regel auszugehen, wenn Personen überwacht werden, die den Gehweg oder die Straße vor einem Grundstück passieren, ohne Anlass für ihre Überwachung gegeben zu haben.

4.48 Zu viele Augen beim Augenarzt – Videogaga 47

Durch eine anonyme Beschwerde wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam, dass in einer Augenarztpraxis eine Videoüberwachung durchgeführt wurde. Neben der Eingangstür zur Praxis war ein großes Schild angebracht, auf dem vermerkt war, dass die Praxis Tag und Nacht videoüberwacht wird. Nachdem sich der TLfDI an die Praxis wandte, teilte diese mit, dass insgesamt 12 Kameras zum Einsatz kämen. Aus den überreichten Unterlagen war erkennbar, dass zwar keine Behandlungsräume videografiert wurden, jedoch die Flure und der Empfangsbereich der Praxis sowie Teile des Wartezimmers. Die verantwortliche Stelle teilte mit, dass die Videoüberwachung zur Wahrnehmung des Hausrechts sowie zur Wahrung berechtigter Interessen nach § 6b Bundesdatenschutzgesetz (BDSG) durchgeführt werde.
Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrechern, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich die Gefährdung ergibt. Derartige Nachweise konnten von der Praxis nicht erbracht werden. Der TLfDI legte gegenüber der verantwortlichen Stelle dar, dass, sofern die Praxis in Betrieb ist, die dort anwesenden Bediensteten einen Diebstahl nicht verhindern könnten, wenn die Aufzeichnungen an einer anderen Stelle auf einer so genannten Black-Box aufliefen. Für den verfolgten Zweck wäre während der Betriebszeit eine Beobachtung im Wege des Live Monitorings ausreichend gewesen. Die Videoüberwachung war daher während der Betriebszeit der Augenarztpra-

xis nicht erforderlich. Zudem überwogen während der Geschäftszeit die schutzwürdigen Interessen der Betroffenen. Aufgezeichnet wurden alle Patienten, die sich in der Praxis aufhielten und sich im Aufnahmebereich der jeweiligen Kamera bewegten. Nach den vorgelegten Screenshots der Kameras waren die Personen auf den Bildern gut zu erkennen. Ärzte erheben dabei unter Umständen auch besondere Arten von personenbezogenen Daten, § 3 Abs. 9 BDSG. Diese unterliegen einem besonderen gesetzlichen Schutz. Nach mehrmaligem Schriftwechsel stellte die verantwortliche Stelle in Aussicht, dass sämtliche Kameras in den Bereichen, in denen sich Patienten aufhalten, nur noch außerhalb der Praxisöffnungszeiten eingeschaltet werden.

Dies allein war für den TLfDI aber nicht ausreichend. Er forderte die Vorlage der technischen und organisatorischen Maßnahmen, die im Hinblick auf die Videoüberwachung getroffen wurden. Denn die verantwortliche Stelle hat vor Beginn der Videoüberwachung den konkreten Zweck der Überwachungsmaßnahme schriftlich festzulegen. Der Zweck ist dabei für jede Kamera einzeln schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG. Es bedarf außerdem schriftlicher Festlegungen dazu, unter welchen Voraussetzungen durch wen Einsicht in die Aufnahmen genommen werden darf und auf welche Weise eine Protokollierung der Einsichtnahme sichergestellt ist.

Besonders interessant war im vorliegenden Fall, dass sich das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) einschaltete und nähere Auskunft zu dem Verfahren verlangte. Der TLfDI erwiderte, dass er für diese Frage unter Zugrundelegung der Regelung des § 36 Abs. 1 Satz 1 Thüringer Datenschutzgesetz keine Zuständigkeit des Ministeriums erkennen könne. Der TLfDI führt ein Verwaltungsverfahren im Sinne von § 9 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) in Verbindung mit § 38 Abs. 1 BDSG durch. Die Beteiligten eines Verwaltungsverfahrens sind in § 13 Abs. 1 ThürVwVfG abschließend aufgeführt. Ein Beteiligter kann sich auch durch einen Bevollmächtigten vertreten lassen, § 14 Abs. 1 Satz 1 ThürVwVfG. Da eine entsprechende Bevollmächtigung nicht vorlag, konnte keine Auskunft erteilt werden. Das TMASGFF wurde gefragt, aufgrund welcher Rechtsgrundlage es die gewünschte Auskunft begehrt und inwieweit die Auskunft für die dortige Aufgabenerfüllung erforderlich ist. Nach § 19 Abs. 1 Thüringer Datenschutzgesetz dürfen öffentliche Stellen

personenbezogene Daten nur erheben, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Soll die Videoüberwachung vor Diebstählen und Vandalismus schützen, ist hierin ein berechtigtes Interesse zu sehen, wenn konkrete Tatsachen die Gefährdung belegen. Sofern von der Videoüberwachung besondere Arten von Daten, wie beispielsweise Daten über die Gesundheit, betroffen sind, ist deren Schutzwürdigkeit im Rahmen der Interessenabwägung bei § 6b BDSG besonders zu berücksichtigen.

4.49 Tabu: Pause! Videogaga 48

Videoüberwachung war auch Thema bei der Kontrolle eines in der Lebensmittelbranche tätigen Produktionsunternehmens. Neben einer umfangreichen Videoüberwachung innerhalb der Produktionsgebäude waren auch außerhalb des Gebäudes Videokameras angebracht. Dabei muss zunächst darauf hingewiesen werden, dass es sich um ein Unternehmen handelte, welches den Datenschutz ernst nimmt. Dies war bereits daran erkennbar, dass die Videoüberwachung innerhalb des Gebäudes vorbildlich eingerichtet war. Eine Arbeitnehmerüberwachung fand nicht statt. Alle Bereiche in denen sich Arbeitnehmer aufhalten und aufhalten könnten, waren geschwärzt und damit bereits vom Aufzeichnungsvorgang ausgeschlossen. Die Überwachung richtete sich allein auf die Produktion und ist damit zulässig. Für die Kontrollierenden, die eher weitgehende datenschutzrechtliche Verstöße gewöhnt sind, sehr ungewohnte Umstände. Allerdings sind auch in diesem Betrieb Mängel festgestellt worden: Im Zuge der Einführung eines betriebsweiten Rauchverbots außerhalb des Unternehmens war ein Unterstand für Raucher eingerichtet worden. Leider wurde dabei nicht bedacht, dass sich dieser im Aufnahmebereich der Außenkameras befindet. Pausenräume für Arbeitnehmer dürfen selbstverständlich nicht überwacht werden, auch wenn dies aus Versehen geschieht. Ebenfalls war die Aufzeichnungsdauer der gesamten Videoüberwachung zu lang gestaltet. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat das Unternehmen nach der durchgeführten Kontrolle auf die Missstände aufmerksam gemacht. Das Unternehmen hat diese sofort korrigiert.

Im Regelfall ist die dauerhafte Videobeobachtung von Arbeitnehmern unzulässig. Dies gilt insbesondere für Rückzugsräume. Dabei kommt es auch nicht darauf an, ob die Videokamera zu diesem Zweck eingerichtet worden ist. Die theoretische Möglichkeit der Beobachtung reicht für einen Verstoß aus.

4.50 Der Spion am Hauseingang – Videogaga 49

Aufgrund eines Hinweises erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, dass wieder einmal an einem Wohngebäude eine Kamera angebracht war. Der TLfDI schrieb daraufhin den Eigentümer des Wohngebäudes an. Dieser teilte mit, dass die Kamera Bestandteil einer Klingel-Sprechanlage sei. Das System sei fachmännisch installiert worden. Weiterhin sei die Kamera nur kurzfristig mit Betätigung der Klingel aktiviert. Die Kamera sollte den Mietern des Wohngebäudes die Möglichkeit verschaffen, durch eine zeitlich begrenzte Bildübertragung die klingelnden Besucher zu identifizieren und über deren Einlass in das Haus zu entscheiden. Grund sei die zwischen Gartentor und Hauseingangstür 70 Meter lange Einfahrt. Durch die Kamera erfolgte keine Aufzeichnung oder Speicherung der Bilder, lediglich die Bewohner des Wohngebäudes hatten Zugriff auf die Klingelanlage.
Im Ergebnis stellte der TLfDI fest, dass die betriebene Kamera mit dem Bundesdatenschutzgesetz (BDSG) vereinbar war. Nach § 6b Abs. 1 Nr. 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Anwendung des § 6b BDSG setzt zunächst voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückeigentümers) von jedermann genutzt oder betreten werden dürfen. Zum öffentlich zugänglichen Raum zählt auch der jedermann zugängliche Eingangsbereich einer privaten Haus- oder Wohnungstür, wie in diesem Fall. Die Videoklingelanlage diente dem Zweck, nur solchen Personen Einlass in das Haus zu gewähren, über deren Identität oder Lauterkeit sich der Hausrechtsinhaber vergewissert

hat. Dies kann nicht durch mildere, ebenfalls geeignete Mittel erreicht werden. Auch stehen keine überwiegenden Interessen des die Klingel betätigenden Besuchers entgegen, wenn die – zeitlich eng begrenzte – Bildübertragung allein zum Zwecke seiner Identifizierung und zur Einlasskontrolle durch den angeklingelten Hausbewohner erfolgt. So entschied der Bundesgerichtshof (BGH) in seinem Urteil vom 8. April 2011 – Az. V ZR 210/10. Danach ist es zulässig, eine Klingelkamera zu betreiben, bei der die Kamera sich nur dann anschaltet, wenn die Klingel betätigt wird. Zudem darf das Video-Bild nur in der Wohnung zu sehen sein, in der auch geklingelt wurde. Dem Mieter wird das Recht zugesprochen, sich zu informieren, wer an seiner Tür klingelt. Dabei sollte die Kamera so eingestellt sein, dass möglichst wenig öffentlich zugängliche Bereiche erfasst werden, sondern vor allem die klingelnde Person gezeigt wird.
Zudem sollte an der Klingel eine Information darüber angebracht sein. Gerade solch ein Hinweisschild nach § 6b Abs. 2 BDSG auf die durchgeführte Videoüberwachung fehlte hier. Der Hinweis ist so anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen. Der TLfDI forderte daraufhin den Eigentümer des Wohngebäudes auf, ein Hinweisschild nachzurüsten. Dieser zeigte sich einsichtig und teilte dem TLfDI mit, dass er ein entsprechendes Hinweisschild bestellt habe.

Laut Urteil des BGH vom 8. April 2011 – Az. V ZR 210/10 ist es zulässig, eine Klingelkamera zu betreiben, bei der die Kamera sich nur dann anschaltet, wenn die Klingel betätigt wird. Das Video-Bild darf aber nur in der Wohnung zu sehen sein, in der auch geklingelt wurde. Dem Mieter wird das Recht zugesprochen, sich zu informieren, wer an seiner Tür klingelt. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch

geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mithilfe entsprechender Schilder erfolgen.

4.51 TLfDI – ach du Schreck, da sind die Kameras einfach weg – Videogaga 50

Ein Mieter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil im Flur und im Aufzug des von ihm bewohnten Mietshauses eine Videoüberwachung durchgeführt wurde. Er habe sich telefonisch und auch schriftlich an seinen Vermieter gewandt, um nähere Auskunft zu erlangen. Dieser teilte ihm mit, dass mit den Videokameras der Zweck verfolgt werde, Sachbeschädigungen im Wohngebäude zu verhindern. In der Vergangenheit sei es gehäuft zu Vandalismus im Personenaufzug und Beschädigungen der Briefkastenanlage gekommen. Auch Mieterpost sei gestohlen worden. Die Aufzeichnungen würden nach einer Woche gelöscht und es werde im Aufzug, im Aufzugsvorraum und an der Hauseingangs- und Kellertür auf die Videoüberwachung hingewiesen.
Der TLfDI wandte sich schriftlich an den Vermieter, um den Sachverhalt weiter aufzuklären. Das Unternehmen teilte mit, dass in dem betreffenden Wohnhaus keine Videoüberwachung installiert sei. Der TLfDI übersandte dem Unternehmen daraufhin die vom Beschwerdeführer überlassenen Fotos von den Kameras und den Hinweisschildern, selbstverständlich, ohne dessen Namen zu nennen. Der Vermieter wurde für den Fall, dass es sich bei den auf den Fotos zu sehenden Kameras um Attrappen handeln sollte, auf Folgendes hingewiesen: Das einschlägige Bundesdatenschutzgesetz hat den Zweck, das Grundrecht auf informationelle Selbstbestimmung zu gewährleisten. Dieses vom Bundesverfassungsgericht in seiner Entscheidung zur Volkszählung vom 15. Dezember 1983 weiterentwickelte Grundrecht auf informationelle Selbstbestimmung beinhaltet auch einen Schutz gegen Kameraattrappen. Dies begründet sich in dem von solchen Einrichtungen ausgehenden Überwachungsdruck. Das Bundesverfassungsgericht hat in seiner Entscheidung 1 BvR 209/83 u. a. vom 15. Dezember 1983 festgestellt, dass eben wesentlicher Inhalt der informationellen Selbstbestimmung der ist, dass dem Einzelnen bekannt ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Genau dies ist bei einer Kameraattrappe nicht gewährleistet, da für jeden unbeteiligten Dritten der Eindruck

erweckt wird, aufgenommen zu werden. Nach Auffassung des TLfDI beurteilen sich Attrappen daher grundsätzlich nach den gleichen Maßstäben wie tatsächlich funktionsfähige Kameras.
Da der potentielle Aufnahmebereich der eingesetzten „Kameras“ der öffentlich zugängliche Eingangsbereich des Wohnhauses war, müssen die Voraussetzungen des § 6b Bundesdatenschutzgesetz vorliegen. Das Unternehmen antwortete, dass weder eine Kamera noch eine Kameraattrappe in dem Wohnhaus installiert sei. Der betriebliche Datenschutzbeauftragte (bDSB) des Unternehmens habe sich persönlich vor Ort davon überzeugt, dass keine Schilder mit dem Hinweis auf Videoüberwachung im Hauseingangsbereich, im Hausflur oder der Tür neben dem Aufzug angebracht sind. Es wurden Lichtbildaufnahmen des Eingangsbereiches sowie des Aufzugsvorraumes übersandt, auf denen weder eine Kamera noch Hinweise auf die Videoüberwachung zu erkennen waren. Da sich der Sachverhalt nachträglich nicht mehr aufklären ließ, erklärte der TLfDI die Angelegenheit für erledigt.

Auf Attrappen sind grundsätzlich die gleichen Maßstäbe anwendbar wie auf tatsächlich funktionsfähige Kameras, weil von ihnen der gleiche Überwachungsdruck ausgeht. Es kann vorkommen, dass Kameras von selbst verschwinden, wenn der TLfDI sich einschaltet.

4.52 Und weg mit den Kameras – Videogaga 51

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) hat eine Privatperson darauf aufmerksam gemacht, dass an einem Gebäude im Südwesten von Erfurt eine Videoüberwachungsanlage angebracht sei, die ausschließlich öffentlich zugängliche Bereiche erfasse.
Die Zulässigkeit einer Videoüberwachung von öffentlich zugänglichen Bereichen hat der Gesetzgeber ausdrücklich und abschließend geregelt. Gemäß § 6b Bundesdatenschutz (BDSG) ist diese nur in engen Grenzen zulässig, beispielsweise dann, wenn hiermit das Hausrecht der verantwortlichen Stelle durchgesetzt werden soll. Aber selbst dann dürfen keine Anhaltspunkte vorhanden sein, dass schutzwürdige Interessen Betroffener überwiegen. Ist dies der Fall, ist auch die Videoüberwachung zum Zweck des Hausrechts unzulässig.

Da es sich nach Überprüfung des TLfDI im konkreten Fall um ein Mehrfamilienhaus handelte und nicht aufklärbar war, welcher Mieteinheit die Videoüberwachung zuzuordnen war, wurden über das zuständige Grundbuchamt zunächst sämtliche Eigentümer des Gebäudes angeschrieben. Diese nahmen fast ausnahmslos das Anliegen des TLfDI sehr ernst. Jedoch war auch den Eigentümern nicht bekannt, wer die Videoüberwachungsanlage installiert hatte. Erst die durch die Eigentümergemeinschaft beauftragte und nunmehr auch dem TLfDI bekannte Immobilienverwaltungsgesellschaft konnte dies auf Nachfrage mitteilen. Auch konnte das weitere Vorgehen durch die Verwaltungsgesellschaft erheblich beschleunigt werden, indem diese den Mieter unter kurzer Fristsetzung zum Abbau der Videokameras aufforderte. Dieser Aufforderung kam der Mieter auch nach.
Ein weiteres Handeln des TLfDI war daher nicht angezeigt.

Auch Privatpersonen, die nicht gewerblich handeln, fallen unter gewissen Umständen in den Anwendungsbereich des BDSG. Dies ist insbesondere oft dann der Fall, wenn öffentlich zugängliche Räume mit Kameras beobachtet oder gar aufgenommen werden. In solchen Fällen ist der TLfDI dann die zuständige Aufsichtsbehörde zur Prüfung, ob diese Anlagen mit dem BDSG vereinbar sind.

4.53 Die Kameras machen Arbeit – Videogaga 52

Die Arbeitnehmer eines Unternehmens wandten sich anonym an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Das Unternehmen hatte am Schwarzen Brett die Videoüberwachung der Fertigungsanlagen angekündigt und sich dabei auf die Gewerbeordnung, spezifische Branchenregelungen und Arbeitsschutzbestimmungen berufen. Die Arbeitnehmer fanden die Videoüberwachung nicht hinreichend begründet und baten den TLfDI um Prüfung.
Der TLfDI wandte sich schriftlich an das Unternehmen und erfragte nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) alle notwendigen Informationen zur Videoüberwachung. Bei der Videoüberwachung werden personenbezogene oder -beziehbare Daten verarbeitet, § 3 Abs. 1 BDSG. Es sollte mitgeteilt werden, wie viele Kameras in dem Unternehmen in welchen Bereichen betrieben werden. Der Zweck sollte für jede Kamera gesondert aufgeführt werden. Der

TLfDI forderte auch die Übersendung der zur Videoüberwachung getroffenen technischen und organisatorischen Maßnahmen nach § 9 BDSG, beispielsweise zur Speicherdauer und zu den Zugriffs- und Auswertungsrechten. Wichtig ist, um eine Vorortkontrolle zu vermeiden, die Vorlage eines Lageplans, aus dem die Grundstücks- und Gebäudebegrenzungen, die Zweckbestimmung der Gebäude, die Nutzungsart des angrenzenden öffentlichen Bereichs (z. B.: Straße, Fußweg, Anlage), Standort der Videokameras einschließlich der jeweiligen Aufnahmebereiche und alle Standorte der Hinweisschilder erkennbar sind sowie ein Ausdruck des von der jeweiligen Kamera erstellten Bildes (Screenshot), aus dem sich der Blickwinkel der Kamera beurteilen lässt.
Der Geschäftsführer des Unternehmens teilte pauschal mit, dass die insgesamt zum Einsatz kommenden Kameras zur Überwachung der technologischen Prozesse einschließlich aller sicherheitsrelevanten Aspekte auch zum Arbeitsschutz, zur Schadensvermeidung und zum Diebstahlschutz erforderlich seien. Solche pauschalen Angaben genügen nicht für eine hinreichende Auskunftserteilung an den TLfDI. Er muss aufgrund der gemachten Angaben in der Lage sein, die datenschutzrechtliche Zulässigkeit jeder einzelnen Kamera prüfen zu können. Daher sind die erforderlichen Angaben für jede Kamera einzeln zu machen. Um den verantwortlichen Stellen diese Angaben zu erleichtern, hat der TLfDI das im Anhang beigefügte Erfassungsblatt für Videokameras entwickelt (siehe Anlage 1).
Das Unternehmen hat daraufhin eine Fristverlängerung beantragt, da die Zusammenstellung aller Unterlagen einige Zeit erfordert. Sobald die nötigen Unterlagen vorliegen, wird der TLfDI die Prüfung fortsetzen.

Die verantwortliche Stelle hat vor Beginn der Videoüberwachung den konkreten Zweck der Überwachungsmaßnahme schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG. Um den Unternehmen diese Aufgabe zu erleichtern, hat der TLfDI ein Erfassungsblatt für Videokameras entwickelt.

4.54 Immer wieder diese Attrappen – Videogaga 53

Aufgrund einer Beschwerde erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis, dass ein Eigentümer auf seinem Grundstück eine Videoüberwachung betrieben hatte. Diese war dazu noch in ihrem Erfassungsbereich auf die angrenzende öffentliche Straße ausgerichtet.
Nachdem sich der TLfDI mit einem Fragenkatalog an den Eigentümer des Grundstücks gewandt hatte, teilte dieser dem TLfDI mit, dass es sich bei den zwei an seinem Haus angebrachten Kameras um solche ohne Anschluss an ein Überwachungsgerät handele. Diese „Imitationen" sollten nur der Abschreckung und der Verhinderung von Diebstählen oder Vandalismus dienen. Mehrfach seien in der Vergangenheit schon Bäume abgesägt und Gartentüren sowie Mülltonnen beschädigt worden. Schließlich sei sogar das Hinweisschild auf die Videoüberwachung im Sinne des § 6b Abs. 2 Bundesdatenschutzgesetz (BDSG) gestohlen worden. Die meisten Fragen des TLfDI wurden jedoch – mit dem Hinweis, es handle sich um Attrappen – nicht beantwortet.
Der TLfDI erteilte dem Eigentümer des Grundstücks den Hinweis, dass die Mitteilung, dass es sich bei den Kameras nur um Attrappen gehandelt habe, nicht die Pflicht zur Beantwortung des vorgenannten umfangreichen Fragenkataloges des TLfDI entfallen ließ.
Denn aufgrund des auch von Attrappen ausgehenden Überwachungsdrucks auf Betroffene und deren mit richtigen Kameras identischer Außenwirkung sind diese nicht anders zu behandeln als funktionierende Kameras. Wegen des ausgeübten Überwachungsdrucks wird ebenfalls in das Persönlichkeitsrecht der betroffenen Personen eingegriffen, da diese nicht wissen, wer wann welche Daten über sie erhoben hat. Hinsichtlich der Zulässigkeit von Kameraattrappen wird auf den Beitrag Nr. 4.27 in diesem Tätigkeitsbericht verwiesen.

Letztendlich teilte der Eigentümer dem TLfDI mit, dass er die zwei Kameraattrappen entfernt habe. Das Verfahren konnte abgeschlossen werden.

Durch den ausgeübten Überwachungsdruck von Kameraattrappen wird ebenfalls in das Persönlichkeitsrecht der betroffenen Personen eingegriffen, da diese nicht wissen, wer wann welche Daten über sie erhoben hat.

4.55 Kein öffentlicher Verkehrsraum – Videogaga 54

Erfreulicherweise meldete sich wieder einmal ein Ordnungsamt beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und gab an, dass an einem Gebäude insgesamt fünf Kameras, die auch den öffentlichen Verkehrsraum erfassten, angebracht seien. Das Ordnungsamt teilte dem TLfDI mit, dass sich ein Bürger aus der Nachbarschaft über die Kameras beschwert habe.
Nach Ermittlung des Sachverhaltes stand fest, dass es sich um eine umfangreiche Videoüberwachung handelte, die auch den öffentlich zugänglichen Bereich miterfasste. Dies ist grundsätzlich nicht zulässig.
Die Aufzeichnung von Bildern stellt eine Datenerhebung dar, die nach § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig ist, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt. Da eine Einwilligung bei Videoüberwachungsanlagen naturgemäß ausscheidet, bleibt es bei der Notwendigkeit einer Rechtsvorschrift.
Maßgebliche Erlaubnisnorm für die Überwachung von öffentlich zugänglichen Räumen ist § 6b BDSG. Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden können.
Die Betreiberin der Kameras benannte als Zweck der Videoüberwachung die Abschreckung, um Graffiti-Vandalismus zu vermeiden bzw. die Beweissicherung zu solchen Taten.
Nach § 6b Abs. 1 BDSG ist eine Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Darüber hinaus prüft der TLfDI, ob an Stelle der Videoüberwachung nicht zumutbare alternative Methoden, die weniger in das Persönlichkeitsrecht der Betroffenen eingreifen, das Ziel der Videoüberwachung mit gleicher Effektivität erreichen. Zum

Beispiel regelmäßige Kontrollgänge von Bewachungspersonal, der Einsatz eines Pförtners oder Hausmeisterdienstes können beispielsweise ebenfalls einen wirksamen Schutz gegen Vandalismus bieten. Das Auftragen von spezieller Oberflächenbeschichtung kann Schutz vor Beschädigungen durch Graffiti bieten.
Bei dem von der Betreiberin angegebenen Zweck handelt es sich um ein berechtigtes Interesse. Allerdings stellte der TLfDI fest, dass hier eine Aufzeichnung für rein präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. Sicherheitspersonal unmittelbar eingreifen kann. Das bedeutet, dass eine reine Videoaufzeichnung zur Verhinderung von Unfällen oder Straftaten nicht geeignet ist.
Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Dies war vorliegend nicht der Fall. Denn die Betreiberin der Kameras teilte dem TLfDI mit, dass sie die zwei auf den Gehweg und somit auf den öffentlich zugänglichen Raum gerichteten Kameras entfernt habe. Eine weitere Kamera habe die Be-treiberin neu ausgerichtet, sodass diese nur noch einen Zufahrtsbereich mit Schranke und damit nur noch das eigene Grundstück erfasste. Damit konnten Fußgänger, die das Grundstück lediglich passierten, aber nicht betraten, nicht mehr in den Aufnahmebereich der Kameras geraten.
Den geforderten Hinweis auf die Videoüberwachung nach § 6b Abs. 2 BDSG brachte die Betreiberin an. Der Hinweis muss so gestaltet und positioniert sein, dass eine Person rechtzeitig erkennen kann, dass sie sich auf einen kameraüberwachten Bereich zubewegt. Die verantwortliche Stelle muss auf dem Hinweisschild genannt werden.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Schließlich hat der Europäische Gerichtshof (EuGH) in seinem Urteil vom 11. Dezember 2014 (Az.: C 212/13) bestätigt, dass auch auf eine

privat betriebene Videoüberwachungsanlage unter bestimmten Voraussetzungen die Europäische Datenschutzrichtlinie und damit das insoweit gleichlautende Bundesdatenschutzgesetz anwendbar ist. Daher fällt jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa weil sie öffentlich zugänglichen Raum erfasst, in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des BDSG.

4.56 Kamera schaut zu tief ins Glas – Videogaga 55 – Videoüberwachung in der Gaststätte

Ein Betroffener trat an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran und teilte mit, dass eine von ihm besuchte Gaststätte seit kurzem im Eingangsbereich wie auch im Inneren videoüberwacht würde. Der TLfDI schrieb daraufhin den Betreiber der Gaststätte mit einem Auskunftsersuchen zur Videoüberwachung an. Es stellte sich heraus, dass in der Gaststätte vier Videokameras betrieben wurden. Eine Kamera überwachte den Eingangsbereich, die drei übrigen Kameras nahmen Teile des Tresens und der Zapfanlage auf. Mit diesen Kameras wurden auch der Sitzbereich vor dem Tresen sowie Tische der Gäste überwacht. Als Grund für die Videoüberwachung wurde angegeben, dass in der Vergangenheit ein TV-Gerät sowie Bilder von der Wand gestohlen worden seien. Darüber hinaus seien ein Portemonnaie sowie ein Barhocker gestohlen worden. Es gebe Zechpreller, diverse Sachbeschädigungen sowie Personenschäden. Die eklatantesten Fälle seien bei der Polizei zur Anzeige gebracht worden. Nachweise hierzu wurden vom Gaststättenbetreiber trotz Aufforderung nicht erbracht. Die Videoaufnahmen wurden sieben Tage von dem Gaststättenbetreiber vor Ort auf einem Server in einem verschlossenen Schrank gespeichert. Der Schlüssel zu diesem Schrank befand sich im Tresor.
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Eine Einwilligung kam im vorliegenden Fall nicht in Betracht. Sie ist nach § 4a Abs. 1 BDSG nur wirksam, wenn sie auf einer freien Entscheidung des Betroffenen beruht und er vorab auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder

Nutzung hingewiesen wurde. Es wurde im Vorfeld keine Einwilligung aller potentiell von der Videoüberwachung Betroffenen eingeholt. Daher bedarf es zur Rechtmäßigkeit der Durchführung der Videoüberwachung einer gesetzlichen Grundlage. Als Erlaubnisnorm kommt ausschließlich § 6b BDSG in Betracht, da es sich bei dem Gastraum einer Gaststätte um öffentlich zugängliche Räumlichkeiten handelt. Unter einem öffentlich zugänglichen Bereich versteht man jeden Raum, der einem unbestimmten Personenkreis zugänglich ist. Die Überwachung solcher Bereiche ist nur im Rahmen einer Erforderlichkeit des abschließenden Zweckkatalogs des § 6b Abs. 1 Nr. 1 bis 3 BDSG zulässig. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit. Derartige Nachweise wurden vom Gaststättenbetreiber nicht erbracht. Es war auch nicht ersichtlich, inwieweit die Videoüberwachung des Eingangsbereichs einer Gaststätte zur Verhinderung von Diebstählen, Sachbeschädigungen und Gewaltdelikten geeignet ist. Die Videoüberwachung war auch nicht so ausgestaltet, dass durch die Überwachung erfasste Vorgänge unmittelbar wahrgenommen werden bzw. auf diese reagiert werden konnte. Da der Gastraum stets mit mehreren Mitarbeitern besetzt ist, lässt sich eine Kontrolle der Gasträume anders realisieren. Damit fehlte es ebenfalls an der Erforderlichkeit der Videoüberwachung, da die Kontrolle durch die Servicemitarbeiter zur Verfolgung des angestrebten Zweckes effektiver ist, weil ein Mitarbeiter ein durch einen Kunden begangenes Fehlverhalten nicht nur besser und zuverlässiger feststellen, sondern auch unmittelbar darauf reagieren kann.

Selbst wenn man die Erforderlichkeit der Videoüberwachung annähme, bestanden Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen überwogen. Betroffene der Überwachung sind insbesondere die Gäste sowie die Bediensteten der Gaststätte. Die Gäste besuchen die Gaststätte vor allem zu Zwecken der Freizeitgestaltung und um sich zu erholen. Das schutzwürdige Interesse der Gäste daran, diesen Aktivitäten ohne eine andauernde Beobachtung durch Videokameras und den dadurch ausgeübten Überwachungsdruck nachzukommen, wird als elementarer Teil des Grundrechts auf in-

formationelle Selbstbestimmung angesehen. Das schutzwürdige Interesse der Gäste an einer von Kameras unbeobachteten Freizeitgestaltung überwiegt insoweit das Interesse des Gaststätteninhabers an der Videoüberwachung der Gäste Dies alleine schon deswegen, da der Bereich der Freizeitgestaltung besonderen Schutz genießt.
Außerdem wurden durch die Kameras Mitarbeiter hinter dem Tresen überwacht, die sich dort ständig bzw. regelmäßig aufhalten, um ihren arbeitsvertraglichen Pflichten nachzukommen. Die Voraussetzungen der nach § 32 Abs. 1 Satz 1 BDSG zulässigen Arbeitnehmerüberwachung waren nicht erfüllt und auch nicht vorgetragen worden. So ist für die Zulässigkeit einer solchen Datenerhebung, -verarbeitung oder -nutzung Voraussetzung, dass diese für Zwecke des Beschäftigungsverhältnisses erfolgt und für dessen Durchführung erforderlich ist. Diese Rechtfertigungsschwelle ist wegen der besonderen Intensität eines durch Videoüberwachung verursachten Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Beschäftigten hoch. Daraus folgt, dass eine präventive Videoüberwachung von Mitarbeitern ohne konkreten Grund den Anforderungen von § 32 Abs. 1 Satz 1 BDSG nicht genügt.
Aus den dargelegten Gründen ordnete der TLfDI mit einem Anordnungsbescheid nach § 38 Abs. 5 Satz 1 BDSG die Demontage der Kameras an. Zum Ablauf des Berichtszeitraums war der Bescheid noch nicht rechtskräftig. Sobald dies der Fall ist, muss der Gaststätteninhaber die Kameras binnen zwei Wochen demontieren. Für den Fall, dass er dieser Anordnung nicht fristgerecht nachkommt, wurde die Festsetzung eines Zwangsgeldes für jede Kamera angedroht. Zudem kann es zu einem Bußgeldverfahren kommen.

Soll eine Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Allerdings überwiegen in aller Regel die schutzwürdigen Interessen der Mitarbeiter, wenn sie sich dauerhaft im Aufnahmebereich der Kamera aufhalten müssen. In diesen Fällen kann der TLfDI die Demontage der Kameras fordern.

4.57 Blick auf den Parkplatz in Sachsen-Anhalt – Videogaga 56

Der Landesbeauftragte für den Datenschutz aus Sachsen-Anhalt gab einen Fall an den Thüringer Landesbeauftragen für den Datenschutz und die Informationsfreiheit (TLfDI) ab. Es handelte sich um eine Beschwerde über die auf dem Außengelände eines Einkaufszentrums in einer Stadt in Sachsen-Anhalt durchgeführte Videoüberwachung. Es hatte sich bei der Prüfung herausgestellt, dass die Stelle, die für die Videoüberwachung zuständig war, der Eigentümer des Geländes mit Sitz in Thüringen war. Glücklicherweise hatte die Behörde in Sachsen-Anhalt bereits eine Vorortkontrolle durchgeführt und Fotografien von den Kameras gemacht. Der TLfDI schrieb den Eigentümer an und übersandte Bilder des Aufnahmebereichs der Kameras. So erübrigte sich eine Kontrolle des TLfDI vor Ort.
Die datenschutzrechtliche Prüfung ergab, dass die Videoüberwachung nur zum Teil zulässig war. Zum Einsatz kamen insgesamt sechs Kameras. Bei der Kontrolle wurden keine Hinweise zur Kenntlichmachung der Videoüberwachung nach § 6b Abs. 2 Bundesdatenschutzgesetz (BDSG) vorgefunden. Als Zweck wurde angegeben, dass es in der Vergangenheit immer wieder zu Beschädigungen des Gebäudes mit Graffiti gekommen sei. Dies wurde auch durch Vorlage entsprechender Fotografien nachgewiesen. Weiterhin wurde angegeben, dass die Aufnahmen auch zur Ermittlung bei Verkehrsunfällen benötigt würden, außerdem müsse der ordnungsgemäße Einsatz eines Dienstleisters, insbesondere bei der Durchführung des Winterdienstes, überprüft werden.
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Da ausschließlich öffentlich zugängliche Bereiche aufgezeichnet werden, müssen die Voraussetzungen des § 6b BDSG erfüllt sein. Danach ist in öffentlich zugänglichen Bereichen die Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein und muss im Hinblick auf den Geschäftszweck des Unternehmens be-

gründbar sein. Dies ist nicht der Fall im Hinblick auf die Absicht der Ermittlung bei Verkehrsunfällen. Nach § 163 Strafprozessordnung (StPO) haben die Behörden und Beamten des Polizeidienstes Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu erlassen, um die Verdunklung der Sache zu verhüten. Die Ermittlung bei Verkehrsunfällen ist daher Sache der Polizei, respektive der Staatsanwaltschaft nach § 160 Abs. 1 StPO. Es ist nicht Aufgabe eines Unternehmens, Ermittlungsbehörden Beweise zur Verfügung zu stellen.
Die Überwachung der ordnungsgemäßen Durchführung des Winterdienstes stellt zwar ein berechtigtes Interesse des Eigentümers dar. Für diesen Zweck ist die Videoüberwachung aber nicht erforderlich. Es wäre ausreichend, wenn die Mieter des Gebäudes vor Ort verpflichtet würden, den Eigentümer zu informieren, wenn das Grundstück nicht ordnungsgemäß beräumt worden ist oder der Dienstleister vor Ort anderen Obliegenheiten nicht ordnungsgemäß nachgekommen ist. Auch die Mieter, die auf den Kundenverkehr angewiesen sind, haben ein Interesse daran, dass das Grundstück ordnungsgemäß beräumt wird.
Soll die Videoüberwachung dazu eingesetzt werden, vor Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn, wie im vorliegenden Fall geschehen, eine tatsächliche Gefahrenlage nachgewiesen werden kann. Allerdings waren nicht alle zum Einsatz kommenden Kameras für den Zweck des Schutzes vor Vandalismus erforderlich bzw. bestanden Anhaltspunkte für das überwiegende schutzwürdige Interesse der betroffenen Personen. Der TLfDI vertrat die Auffassung, dass es für die Beweissicherung im Fall der Sachbeschädigung am Gebäude ausreichen würde, wenn die Gebäudewand und ein davorliegender Teil des Grundstücks, auf dem sich mögliche Täter aufhalten können, aufgezeichnet würden. Es bestand keine Notwendigkeit, den kompletten Parkplatz aufzunehmen. Außerdem ergab eine Abwägung der schutzwürdigen Interessen des Überwachenden mit den schutzwürdigen Interessen der von der Überwachung Betroffenen, dass Letztere überwiegen. Durch die Kamera werden alle auf dem im Aufnahmebild Parkenden aufgezeichnet, ohne dass sie das Eigentum des Grundstückinhabers beeinträchtigen. Es handelt sich also um eine Datenspeicherung auf Vorrat für den Fall, dass jemand das Gebäude schädigen will, auf dem Parkplatz parkt und sich durch verdächtige Umstände als Täter zu

erkennen gibt. Dies kann die Speicherung der Aufnahmen sämtlicher Kunden, die den Parkplatz nutzen, nicht rechtfertigen.
Da der Grundstückseigentümer den Forderungen des TLfDI nicht nachkommen wollte, erließ dieser einen Anordnungsbescheid, indem er dem Grundstückseigentümer aufgab, die Kameras, die zum Schutz vor Vandalismus erforderlich waren, innerhalb von zwei Wochen nach Bestandskraft des Bescheides zu deinstallieren und dies dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit in dieser Frist in geeigneter Weise nachzuweisen. Weiterhin verlangte er, an allen Eingangsbereichen des Grundstücks Hinweise anbringen zu lassen, aus denen sich der Umstand der Beobachtung und die für die Videoüberwachung verantwortliche Stelle erkennen lassen. Da gegen den Bescheid keine Klage erhoben wurde, ist er bestandskräftig geworden. Der Grundstückeigentümer hat signalisiert, dass er den Forderungen des TLfDI nachkommen will und diesem entsprechende Nachweise zukommen lässt. Sollte er dem nicht fristgerecht nachkommen, wird der TLfDI das im Bescheid angedrohte Zwangsgeld festsetzen müssen. Ein anschließendes Bußgeldverfahren drängt sich auf.

Für die Zuständigkeit einer datenschutzrechtlichen Kontrolle einer Datenverarbeitung ist entscheidend, in welchem Bundesland sich die verantwortliche Stelle befindet. Ist eine Videoüberwachung nicht mit den datenschutzrechtlichen Bestimmungen vereinbar, kann der TLfDI die Durchführung von Maßnahmen mit einem Anordnungsbescheid fordern. Diese Forderungen kann er mit der Androhung, Festsetzung und Vollstreckung von Zwangsgeld durchsetzen. Unabhängig davon kann ein Bußgeldverfahren eingeleitet werden.

4.58 Spielhalle im Kameraauge – kein Videogaga 57

Einmal mehr fühlte sich ein Bürger durch installierte Videokameras auf dem Nachbargrundstück belästigt. Im konkreten Fall wurden fünf Kameras von dem Betreiber einer Spielhalle auf seinem Grundstück installiert. Der betroffene Bürger sah die Videokameras als auf den öffentlichen Bereich und sein Grundstück gerichtet an. Er bat deshalb den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Abhilfe. Wie üblich wurde der Spielhallenbetreiber unter Bezugnahme auf die einschlägigen Rechtsgrundlagen (§ 42 Abs. 1 Thüringer Datenschutzgesetz i. V. m.

§ 38 Abs. 6 Bundesdatenschutzgesetz) angeschrieben und um Beantwortung einiger Fragen, z. B. zum Zweck der Videoüberwachung, zur Anzahl der Kameras, ihren Aufnahmebereichen und zur Datenspeicherung um Stellungnahme gebeten. Die Antwort des Spielhallenbetreibers war konstruktiv und umfassend. Als Grund für die Installation der Anlage wurden Sachbeschädigungen am Gebäude angeführt, die zur Anzeige gebracht und polizeilich verfolgt worden waren. Entsprechende Belege hierfür fügte der Spielhallenbetreiber seiner Antwort an den TLfDI bei. Die ebenfalls mitgelieferten Aufnahmen ließen erkennen, dass die Kameras nur Bereiche auf dem Privatgrundstück mit der Spielhalle erfassten. Öffentliche Bereiche wurden nicht erfasst bzw. in der Aufzeichnung geschwärzt. Auch Aufnahmen von Nachbargrundstücken wurden nicht gemacht. Der Betreiber erklärte, dass mit einem Schild am Eingang auf die Videoüberwachung hingewiesen und die Videobilder 14 Tage lang gespeichert werden würden. Der TLfDI klärte den Betreiber darüber auf, dass vor Installation einer Anlage geprüft werden müsse, ob der damit verbundene Zweck auch durch andere Maßnahmen erreicht werden kann, die in die Rechte der Betroffenen weniger stark eingreifen. Der Betreiber legte plausibel dar, dass eine Videoüberwachung mit Aufzeichnung der Videobilder angemessen sei. Andere Maßnahmen wie z. B. die ständige Anwesenheit einer Wachperson auf dem Grundstück oder das Abstellen einer Person zur ständigen Beobachtung von Live-Bildern der Kameras seien unwirtschaftlich und nicht möglich. Der TLfDI bewertete danach den Einsatz der Videoanlage nach § 6b Abs. 2 BDSG als zulässig. Er stellte aber klar, dass eine 14-tägige Speicherung der Videoaufnahmen nicht zulässig im Sinne von § 6b Abs. 5 BDSG sei. Ob eine Verwendung des Materials für eine Beweissicherung notwendig sei oder nicht, könne in ein bis zwei Tagen abgeklärt werden. Grundsätzlich seien deshalb die Videoaufnahmen nach 48 Stunden zu löschen. Zudem übte der TLfDI berechtigte Kritik an Anzahl und Inhalt der Hinweisschilder auf die Videoüberwachung. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Ein Hinweis auf die verantwortliche Stelle fand sich auf den Schildern aber nicht.
Der Betreiber der Videoanlage erklärte daraufhin, die Videodaten zukünftig nach zwei Tagen zu löschen. Ein zweites Schild werde an der Rückseite des Gebäudes angebracht und die Schilder würden durch die Angabe der verantwortlichen Stelle ergänzt.

Der Vorgang zeigt, dass Betreiber von Videoanlagen durchaus bereit sind, den rechtlichen Argumenten des TLfDI zu folgen, um ihre Anlage datenschutzkonform zu betreiben. Jedenfalls liefern die Kameraaugen an dieser Spielhalle ein weiteres Beispiel dafür, dass Betreiberinteressen und Datenschutz kein Gegensatz sein müssen.

Gemäß § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Ob eine Verwendung des Materials für Zwecke der Beweissicherung notwendig ist oder nicht, kann in aller Regel in ein bis zwei Tagen abgeklärt werden. Videoaufzeichnungen können in diesen Fällen grundsätzlich nach 48 Stunden gelöscht werden. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen.

4.59 Durchblick für den Augenarzt? – Videogaga 58

Darf der Nachbar meine Wohnung und meinen Balkon überwachen? Genau diese Frage stellte sich ein Bürger aus Erfurt. Dieser wohnte in einem Mehrfamilienhaus. Sein Nachbar hatte deutlich sichtbar eine vermeintliche Kamera in seiner Wohnung angebracht. Die Kamera war an der Decke, direkt vor einer Fensterfront, angebracht und überwachte dem ersten Anschein nach die Wohnungen und Balkone der Nachbarn.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) schrieb den Betreiber der Kamera (einen Augenarzt!) an und erklärte, dass die Erhebung von Videoaufnahmen grundsätzlich unzulässig sei, es sei denn, es liegt eine gesetzliche Ermächtigung nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) vor. Weiterhin erhielt der Augenarzt einen umfangreichen Fragenkatalog, um die Überwachungsanlage bewerten zu können. Die Antwort ließ nicht lange auf sich warten. Darin wurde dargelegt, dass die Kamera Bestandteil einer Einbruchsmeldeanlage sein sollte, aber nie angeschlossen worden war. Die Grundrechtsbeeinträchtigung von einer echten Kamera und einer Attrappe sind identisch. Diese Kamera wäre aufgrund des psychischen Überwachungsdrucks wie eine funktionstüchtige Kamera zu bewerten. Da die Kamera von dem Betreiber umgehend nach Erhalt des Schreibens des TLfDI

entfernt wurde, waren aus datenschutzrechtlicher Sicht keine weiteren Maßnahmen notwendig.

Videokameras und Kameraattrappen erzeugen einen psychischen Überwachungsdruck auf die betroffenen Personen. Daher sind die Grundrechtsbeeinträchtigungen von echter Kamera und Attrappe identisch zu bewerten.

4.60 Umgeworfene Mülltonnen und Graffiti (Vandalismus) – Videogaga 59

Sie sind Hauseigentümer und haben mit Graffiti-Schmierereien zu kämpfen? Dann wissen Sie, wie schwierig es ist, die Verantwortlichen zur Verantwortung zu ziehen. Ein Hauseigentümer, gleichzeitig Kamerabetreiber, hatte zum Schutz vor Vandalismus eine Kamera an seinem Hauseingang angebracht. Der Hauseigentümer hatte einen Fahrraddiebstahl, mehrere Graffiti-Schmierereien, umgeworfene Mülltonnen und herausgerissene Blumenkästen zu verzeichnen. Danach hatte er eine Kamera am Hauseingang angebracht, die seit der Anzeige des Beschwerdeführers schon seit über einem Jahr nicht mehr in Betrieb und somit eine Attrappe war. Da Videoattrappen wegen des erzeugenden Überwachungsdrucks genauso wie funktionstüchtige Kameras zu bewerten sind, hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) diese Kamera genauer unter die Lupe genommen.
Eine Videoüberwachung zur Wahrnehmung des Hausrechts kann neben der Beobachtung zu präventiven Zwecken auch als repressives Mittel zur Beweissicherung eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung zivilrechtlicher Schadensersatzansprüche zu ermöglichen (Scholz in Simitis, Bundesdatenschutzgesetz, 8. Auflage, § 6b, Rn. 75). Die von dem Hauseigentümer angebrachte Videoüberwachung war erforderlich, um weitere Vandalismus-Schäden abzuwenden. Nach Installation der Videoüberwachungsanlage konnten keine weiteren Beschädigungen und Diebstähle festgestellt werden. Der Hauseigentümer hatte alle Beschädigungen der Polizei gemeldet und dem TLfDI hinreichend nachgewiesen. Nach Prüfung der Kamera konnte festgestellt werden, dass das Schutzbedürfnis des Kamerabetreibers an seinem Eigentum den Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen überwog. Diesen sind die genaueren Umstände der Vi-

deoüberwachung in aller Regel unbekannt. Die Betroffenen können die Eingriffsintensität der Videoüberwachung daher nicht verlässlich einschätzen. Eine Minimaltransparenz schafft § 6b Abs. 2 BDSG: Der Umstand der Videobeobachtung und die verantwortliche Stelle sind hiernach durch geeignete Maßnahmen erkennbar zu machen. Die Betroffenen müssen ohne Weiteres eine Vorstellung bekommen können, wo und wann sie von der Kamera erfasst werden. Der Hinweis auf die verantwortliche Stelle erfordert die vollständige namentliche Nennung der nach § 3 Abs. 7 BDSG verantwortlichen Stelle. Auf weitergehende Angaben zur Identifizierung, wie etwa Postanschrift und die Angabe eines konkreten Ansprechpartners, kann allenfalls dann verzichtet werden, wenn diese Informationen offenkundig sind. Dies ist aber bei Eigentümern und Mietern des Hauses, an dem die Kamera installiert ist, regelmäßig nicht der Fall.
Nach mehrmaliger Aufforderung des TLfDI hatte der Hauseigentümer ein Hinweisschild zur Videokamera angebracht, das den Anforderungen des § 6b BDSG genügt.

Ob und in welchem Ausmaß eine Videoüberwachungsanlage zulässig ist, bedarf immer einer Einzelfallprüfung. Da von Kameraattrappen der gleiche psychische Überwachungsdruck ausgeht wie von einer funktionstüchtigen Kamera, sind diese datenschutzrechtlich ebenso zu bewerten und die daraus entstehenden Pflichten sind vom Betreiber der Videokamera zu erfüllen.

4.61 Auskunftserteilung auch bei Kameraattrappen!

Eine besorgte Bürgerin fühlte sich in ihrer Privatsphäre gestört, weil ihr Nachbar zwei Videokameras an seinem Haus angebracht hatte. Sie vermutete, dass die Kameras auch ihr eigenes Wohnzimmer aufzeichneten. Bei der Prüfung des Sachverhalts hatte der Nachbar angegeben, dass es sich um ausgemusterte Vorführgeräte handele, welche nicht in Betrieb sind und nur als Attrappe zur Abschreckung angebracht wurden. Der Nachbar hatte sich darauf berufen, die Fragen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nicht beantworten zu müssen, da es sich „nur“ um eine Kameraattrappe handelte. Die Pflicht zur Beantwortung der gestellten Fragen entfällt schon nicht, weil Attrappen nicht anders zu behandeln sind als funktionierende Kameras. Jedenfalls insoweit nicht, wie die Fragen auch auf Attrappen anwendbar

sind. Eine Frage zum Speichermedium muss bei einer Attrappe nicht beantwortet werden. Die Frage nach der Ausrichtung hingegen schon. Attrappen erzeugen den gleichen Überwachungsdrucks auf die betroffenen Personen wie eine funktionierende Kamera. Durch den ausgeübten Überwachungsdruck wurde ebenfalls in das Persönlichkeitsrecht der betroffenen Bürgerin eingegriffen, da diese nicht wusste, wer wann welche Daten über sie erhoben hat (vergleiche auch BVerfG Urteil vom 15. Dezember 1983, Az.: 1 BvR 209/83). Der Nachbar sollte dem TLfDI weiterhin einen Lageplan vorlegen, aus dem sich die Ausrichtung der Kameras ergab.

Der Betreiber der Kamera reagierte im Berichtszeitraum noch nicht auf die Forderungen des TLfDI. Zur Erreichung der notwendigen Informationen, um diesen Sachverhalt zu überprüfen, wird sich der TLfDI mit einem förmlichen Auskunftsverlangen nach § 38 Abs. 3 BDSG an den Betreiber wenden. Gegebenenfalls wird ein Zwangs- und Bußgeldverfahren wegen mangelnder Unterstützung des TLfDI eingeleitet werden, sofern der Kamerabetreiber kein Auskunftsverweigerungsrecht wegen einer drohenden Ordnungswidrigkeit hat und sich auf dieses beruft.

Der TLfDI hat als zuständige Aufsichtsbehörde die Mittel der Anordnung unter Androhung eines Zwangsgeldes, wenn ihm Auskünfte nicht erteilt werden, die den Betroffenen nicht in die Gefahr einer Ordnungswidrigkeit bringen. Parallel dazu kann der TLfDI von der Möglichkeit Gebrauch machen, ein Ordnungswidrigkeitenverfahren einzuleiten.

4.62 Einmal ist keinmal – Videogaga 60

Eine Stadtverwaltung leitete dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Eingabe eines Bürgers über eine privat installierte Überwachungskamera, ausgerichtet auf öffentlich zugänglichen Raum, weiter. In dieser beschwerte sich ein Bürger darüber, dass eine auf dem Balkon angebrachte Kamera auf den öffentlichen Gehweg sowie auf angrenzende Grundstücke der Gemeinde ausgerichtet sei.
Mit einem umfassenden Fragenkatalog forderte der TLfDI den Betreiber der Kamera zur Auskunft im Sinne des § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) zum Sachverhalt auf. Der Betreiber teilte

dem TLfDI mit, dass es sich bei der streitgegenständlichen Kamera lediglich um einen Dummy gehandelt habe, sodass es seiner Meinung nach einer Beantwortung des umfassenden Fragenkataloges nicht mehr bedurfte. Dem ist jedoch nicht so: Denn aufgrund des auch von Attrappen ausgehenden Überwachungsdrucks auf Betroffene und deren mit richtigen Kameras identischer Außenwirkung, sind diese nicht anders zu behandeln als funktionierende Kameras. Durch den ausgeübten Überwachungsdruck wird ebenfalls in das Persönlichkeitsrecht der betroffenen Personen eingegriffen, da diese nicht wissen, wer wann welche Daten über sie erhoben hat. Hinsichtlich der Zulässigkeit solcher Kameraattrappen wird auf Nummer 4.27 dieses Tätigkeitsberichts verwiesen. Demnach erteilte der TLfDI dem Betreiber den Hinweis, dass die Pflicht zur Beantwortung der gestellten Fragen nicht entfällt, nur weil die streitgegenständliche Kamera eine Attrappe war.
Dies führte dazu, dass der Betreiber dem TLfDI anzeigte, dass er die Kameraattrappe auf dem Balkon entfernt habe. Um das zu überprüfen, hat der TLfDI die Stadtverwaltung im Rahmen der Amtshilfe um eine Vorortkontrolle gebeten. Nach erfolgter Prüfung der Vollzugsdienststreitkräfte der Abteilung Stadtordnungsdienst und Bußgeldangelegenheiten, ob der Betreiber die streitgegenständliche Attrappe entfernt habe, stellten diese bei der Vorortkontrolle Folgendes fest: Die Videoüberwachungsanlage am Balkon war nicht mehr vorhanden, dafür befand sich nun eine Videoüberwachungsanlage am Carport, ausgerichtet auf die Einfahrt des Grundstücks. Dies konnten die Vollzugsdienststreitkräfte dem TLfDI auch an Hand von Fotos dokumentieren.
Daraufhin schrieb der TLfDI den Betreiber erneut mit der Bitte um Stellungnahme zu der Kamera am Carport an. Das Verfahren ist noch nicht abgeschlossen. Über den Ausgang wird der TLfDI im nächsten Tätigkeitsbericht berichten.

Kameraattrappen sind nur insoweit zulässig, wie auch eine funktionstüchtige Kamera zulässig wäre. Denn auch hier ist der Überwachungsdruck der gleiche wie bei einer funktionstüchtigen Kamera. Dies bestimmt sich bei Kameras, die auf öffentlich zugänglichen Raum ausgerichtet sind, in der Regel nach § 6b BDSG.

4.63 Schloss im Fokus – Videogaga 61 – Videoüberwachung im Museum

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil in einem Schloss nicht nur Museumsführungen für Besucher angeboten, sondern auch Videoaufzeichnungen von diesen angefertigt werden würden. Das Schloss sei mit zwei Kameras an der Hauswand ausgestattet. Die Angaben bestätigten sich, nachdem der TLfDI die Betreiber mit einem umfassenden Fragenkatalog anschrieb. Die Betreiber antworteten dem TLfDI, dass keine Videoüberwachungsanlage betrieben würde, vielmehr handele es sich um zwei Kameraattrappen, welche sie zum Schutz vor Vandalismus angebracht hätten. Mehrfach sei in der Vergangenheit die Fassade des Hauses durch Graffiti-Schmierereien sowie Farbbomben in Mitleidenschaft gezogen worden.
Der TLfDI wird die Videoattrappen, wegen des gleichen Überwachungsdrucks wie bei funktionstüchtigen Kameras, genauer unter die Lupe nehmen.
Wegen dieses gleichen Beobachtungsdrucks sind Attrappen nur unter denselben Bedingungen zulässig, die auch eine echte Kamera erfüllen muss. Nach dem Willen des Gesetzgebers muss die in weiten Bereichen von nicht-öffentlichen Stellen bereits durchgeführte Videoüberwachung öffentlich zugänglicher Räume auf eine gesetzliche Grundlage gestützt werden, die der Wahrung der informationellen Selbstbestimmung durch einen angemessenen Interessenausgleich Rechnung trägt. Im Fall von öffentlich zugänglichen Räumen regelt § 6b Bundesdatenschutzgesetz (BDSG) die Zulässigkeit solcher Kameras. Eine Videoüberwachung zur Wahrnehmung des Hausrechts kann neben der Beobachtung zu präventiven Zwecken auch als repressives Mittel zur Beweissicherung eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung zivilrechtlicher Schadensersatzansprüche zu ermöglichen, wenn sie hierfür erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Dritter überwiegen.
Nach derzeitiger Aktenlage könnten die angebrachten Kameraattrappen in diesem Fall zulässig sein. Bisher konnten die Betreiber dem TLfDI alle Beschädigungen durch Fotodokumentation hinreichend nachweisen. Darüber hinaus seien die Vorkommnisse auch der Polizei sowie der Versicherung gemeldet worden. Daher könnte vorlie-

gend das Schutzbedürfnis der Kamerabetreiber an deren Eigentum den Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen überwiegen.
Über den Ausgang des Verwaltungsverfahrens wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Die Zulässigkeit einer Videoüberwachungsanlage stellt immer eine Einzelfallprüfung dar. Da von Kameraattrappen der gleiche psychische Überwachungsdruck ausgeht wie von einer funktionstüchtigen Kamera, sind diese datenschutzrechtlich ebenso zu bewerten und die daraus entstehenden Pflichten vom Betreiber der Videokamera zu erfüllen.

4.64 Videokamera pro Denkmalschutz – Videogaga 62

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde darauf aufmerksam gemacht, dass eine Videoüberwachungsanlage einen Gehweg filme. Ein Bürger fühlte sich in seinem Persönlichkeitsrecht auf informationelle Selbstbestimmung beeinträchtigt. Die gemeldete Videoüberwachungsanlage wurde umfangreich geprüft. Es wurde festgestellt, dass sich an einem unter Denkmalschutz stehenden Gebäude mehrere Kameras befanden. Alle Kameras zeichneten nur in den Nachtstunden Bilder auf.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist eine Videoüberwachung grundsätzlich, wie jeder Umgang mit personenbezogenen Daten, nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnungen von einer gesetzlichen Vorschrift erlaubt werden. Eine Videoüberwachungsanlage gemäß § 6b BDSG zur Wahrnehmung des Hausrechts ist dann erforderlich, wenn eine tatsächliche Gefahrenlage nachgewiesen wird und auch zukünftig schwerwiegende Beeinträchtigungen drohen. Die verantwortliche Stelle hatte dem TLfDI Schmierereien an der Grundstücksmauer mit Bildern nachgewiesen und die polizeilichen Tagebuchnummern dazu angegeben. In den Bereichen, in denen eine Videoüberwachungsanlage betrieben wurde, konnten seit Inbetriebnahme der Kameras keine neuen Vorfälle von Schmierereien oder Beschädigungen festgestellt werden. Das Haus war ein Einzeldenkmal und unterlag daher einem besonderen Schutz. Die Fassade konnte nur mit hohem Aufwand von den Graffitis befreit werden.

Ein öffentlicher Raum (Gehweg) vor der streitgegenständlichen Fassade wurde mit nicht mehr als einem 1 Meter breiten Streifen aufgezeichnet. Ein Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2013 (Aktenzeichen 16 C 427/02) befand dies als zulässig. Auch bestanden in diesem Fall keine Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwogen. Das Interesse des Eigentümers zum Schutz des denkmalwürdigen Gebäudes wurde höher als das Interesse der Betroffen, nicht videografiert zu werden, beurteilt. Da die Videoaufnahmen nur in den Nachtstunden vorgenommen wurden, war der Kreis der Betroffenen gegenüber einer dauerhaften Aufzeichnung deutlich kleiner, denn der Gehweg vor der Hausfassade war in den Nachtstunden deutlich weniger frequentiert als bei Tage.
Alle Kameras waren als zulässig zu bewerten, nachdem Hinweisschilder angebracht wurden, die den Umstand der Überwachung verdeutlichten und die Speicherdauer der Aufnahmen auf 48 Stunden begrenzt wurde. Das bedeutete aber auch, dass eine Speicherung und Übermittlung der gewonnenen Bilddaten zu einem anderen Zweck als der Täteridentifikation bei Beschädigungen oder Schmierereien an der Hauswand vom Eigentümer ausgeschlossen werden mussten.

Eine Überwachungsanlage kann nur als zulässig bewertet werden, wenn diese auf das erforderliche Maß beschränkt ist, kein milderes Mittel zur Zweckerreichung gegeben ist und die schutzwürdigen Interessen der betroffenen Personen gegenüber den Interessen des Videobetreibers kritisch geprüft wurden. Zudem müssen die Anforderungen des § 6b BDSG an ein Hinweisschild erfüllt und die Speicherdauer auf ein Minimum begrenzt sein.

4.65 Abbau besser als TLfDI im Haus – Videogaga 63

Ein Mitarbeiter einer GmbH meldete sich anonym beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und informierte, dass in der betreffenden Firma im Innen- und Außenbereich insgesamt sieben Kameras installiert worden seien. Der Chef sei zwar im Urlaub, nähme aber in Anrufen Bezug auf Tätigkeiten der Mitarbeiter, von denen er nur durch die Bilder der Videokameras erfahren haben könne.
Der Geschäftsführer der GmbH reagierte lange nicht auf die Bitte des TLfDI, zum Sachverhalt Stellung zu nehmen. Erst nach erneuter

Aufforderung antwortete er zum Fragenkatalog des TLfDI, leider unvollständig. Zur Begründung der Videoüberwachung wurde pauschal der Schutz vor Diebstählen angeführt. Nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Beobachten öffentlich zugänglicher Räume mittels Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn, wie in diesem Fall, in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden, zum Beispiel in Verkaufsräumen. Die vollständige Beantwortung der in einem Auskunftsersuchen enthaltenen Fragen ist die Voraussetzung dafür, dass der TLfDI eine Einschätzung zur Rechtmäßigkeit der Videoanlage vornehmen kann. Daher ist die verantwortliche Stelle nach § 38 BDSG auch verpflichtet, dem TLfDI die erforderlichen Auskünfte zu erteilen. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Diese Nachweise wurden vom Geschäftsführer nicht erbracht. Aufgrund der unvollständigen Stellungnahme und fehlender Belege, zum Beispiel zu den Einbruchs-Vorfällen, die Anlass für die Installation der Videoanlagen waren, musste der Betreiber in den darauffolgenden Monaten erneut mehrfach angeschrieben werden. Letztlich entschied sich der Geschäftsführer, die Anlage außer Betrieb zu nehmen und zu verkaufen mit dem Hinweis auf den aus seiner Sicht zu hohen Klärungsaufwand.

In einer GmbH wurde eine auffällig große Anzahl an Videokameras installiert, durch die sich Mitarbeiter der Firma beobachtet fühlten. Den Klärungsprozess zur Rechtmäßigkeit konnte der TLfDI leider nicht abschließen. Die Anlage wurde vom Betreiber abgebaut, da ihm der Aufwand für die Beantwortung der Fragen des TLfDI zu hoch erschien.

4.66 Die Kontrolle ist oft erst der Anfang – Videogaga 64 – Datenschutz bei Recyclingunternehmen

Bereits im letzten Berichtszeitraum hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) anlassunabhängige Kontrollen bei diversen Recyclingunternehmen durchgeführt. Hierüber wurde unter Nummer 3.11 im 1. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich berichtet. Die Nachbereitung dieser Kontrollen ist in einigen Unternehmen noch nicht abgeschlossen, weil die Herstellung datenschutzgerechter Zustände dort einige Zeit in Anspruch nimmt. In einem Unternehmen gab es beispielsweise keinen betrieblichen Datenschutzbeauftragten (bDSB), die Mitarbeiter, die mit personenbezogenen Daten arbeiteten, waren nicht nach § 5 Bundesdatenschutzgesetz (BDSG) auf das Datengeheimnis verpflichtet, es existierte im gesamten Unternehmen kein schriftliches IT-Sicherheitskonzept, außerdem wurde eine Videoüberwachung durchgeführt, zu der es aber keine schriftlichen Festlegungen gab. Die Forderungen des TLfDI wurden dem Unternehmen in einem kostenpflichtigen Kontrollbericht mitgeteilt. In diesem Fall hatte das Unternehmen die Kosten der Kontrolle zu tragen, da bei der Kontrolle datenschutzrechtliche Mängel festgestellt wurden, § 42 Abs. 4 Satz 2 Thüringer Datenschutzgesetz (ThürDSG). Im aktuellen Berichtszeitraum bemühte sich das Unternehmen, die datenschutzrechtlichen Forderungen umzusetzen. Mittlerweile werden die Mitarbeiter im Unternehmen auf das Datengeheimnis verpflichtet, es gibt einen Datenschutzbeauftragten, es existiert ein schriftliches IT-Sicherheitskonzept, das Regelungen zum Datenschutz, zur Nutzung der Arbeitsplätze mit IT-Unterstützung, zum Umgang mit Telefon, E-Mail und Internet, insbesondere zu deren privater Nutzung, Berechtigungs- und Zugriffsregelungen für Fachanwendungen, Festlegungen zu Passwörtern enthält und vieles mehr.

Im Hinblick auf die Videoüberwachung besteht aber immer noch Klärungsbedarf. Das Unternehmen betreibt zehn Domekameras innerhalb und außerhalb des Firmengebäudes. Eine Domekamera ist eine Überwachungskamera, die unter einer halbrunden getönten Kuppel aus Kunststoff eingebaut ist, weswegen die Kamera und ihre Aufnahmerichtung von außen nicht zu erkennen sind.

Da eine Videoaufzeichnung nicht stattfindet, sondern es lediglich ein Live-Monitoring gibt, das in einem Wachraum live anzusehen ist,

war das Unternehmen der Auffassung, dass weitere Festlegungen wie z. B. zu Zugriffrechten oder zum Zweck der eingesetzten Überwachung nicht zu treffen sind. Diese Auffassung teilt der TLfDI nicht. Auch wenn die Kameras keine Aufzeichnungen vornehmen, handelt es sich um eine Videoüberwachung nach der gesetzlichen Definition des § 6b BDSG. § 6b Abs. 1 BDSG definiert die Videoüberwachung als „Beobachtung" mit optisch-elektronischen Einrichtungen. Der Begriff der Videoüberwachung umfasst damit sowohl die Videobeobachtung, bei der eine Liveübertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Vor Beginn der Videoüberwachung ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen. Zudem sind technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der Daten zu gewährleisten, § 9 BDSG. Daher muss auch bei einer reinen Beobachtung der Zweck jeder Kamera festgelegt werden und die Zugriffsrechte müssen schriftlich festgehalten werden. Dies wurde dem Unternehmen seitens des TLfDI mitgeteilt. Sollte sich das Unternehmen weiterhin weigern, schriftliche Festlegungen zu treffen, wird ihm dies durch einen Anordnungsbescheid aufgegeben werden. Ein Bußgeldverfahren wird sich möglicherweise anschließen.

Auch die reine Videobeobachtung in Form eines Live-Monitorings fällt unter den gesetzlichen Begriff der Videoüberwachung. Damit sind auch auf sie alle gesetzlichen Anforderungen an die Videoüberwachung zu stellen. Insbesondere sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung datenschutzrechtlicher Bestimmungen zu garantieren.

4.67 Kamera vom Grill – Imbiss totalüberwacht – Videogaga 65

Das Ordnungsamt einer Kommune hat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht, dass ein Imbiss, der auf dem Gebiet der Gemeinde betrieben wurde, komplett videoüberwacht würde. Der TLfDI wandte sich mit einem Auskunftsersuchen nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) an den Inhaber des Imbisses. Dieser übersandte in seinem Antwortschreiben Fotos, die offensichtlich von Bildern der Videoüberwachung gemacht wurden. Daraus ließ sich erkennen, dass der Imbiss nahezu komplett videoüber-

wacht wurde. Dies betraf sowohl die Theke, in der die Speisen angeboten wurden, als auch den Gastraum mit den Sitzplätzen der Gäste. Auch die Küche, Teile des Lagers, der komplette Kassenbereich und der Außenbereich des Imbisses wurden überwacht. Neben den Fotos wurde eine allgemeine Begründung zur Videoüberwachung angeführt. Sie diene der Sicherheit des Eigentums und der Sicherheit der Mitarbeiter. Damit gab sich der TLfDI nicht zufrieden. Er wies den Inhaber darauf hin, dass nach § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit ein Gesetz sie erlaubt oder der Betroffene eingewilligt hat. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachung ist § 6b BDSG, wenn öffentlich zugängliche Räume überwacht werden. Dies betrifft Bereiche, die Kunden zugänglich sind. Sofern der Aufnahmebereich in nicht öffentlich zugänglichen Räumen liegt und Beschäftigte bei ihrer Arbeit gefilmt werden, müssen die Voraussetzungen des § 32 BDSG vorliegen. Hieran hatte der TLfDI erhebliche Zweifel. Damit der TLfDI die Zulässigkeit jeder einzelnen Kamera überprüfen konnte, wurde der Inhaber aufgefordert, eine Liste der zum Einsatz kommenden Kameras einzusenden und für jede Kamera gesondert den Zweck ihres Einsatzes zu benennen. Im folgenden Schriftwechsel wies der inzwischen hinzugezogene Rechtsanwalt darauf hin, dass der Imbiss relativ abgelegen liege. Die Fotos wurden zwar näher beschrieben, aber es fehlte wiederum eine genaue Bezeichnung der Kameras, die der TLfDI jedoch benötigt, um möglicherweise Anordnungen zur Videoüberwachung zu treffen. Der Rechtsanwalt musste auf Nachfrage einräumen, dass es bisher im Imbiss trotz der abgeschiedenen Lage zu keinem Eigentumsdelikt gekommen sei. Dies habe aber auch an der Installation der Videokameras gelegen. Der Rechtsanwalt wurde vom TLfDI nochmals aufgefordert, eine Liste der zum Einsatz kommenden Kameras einzusenden. Dieser Forderung ist er im Berichtszeitraum nicht nachgekommen. Vielmehr wurde die Notwendigkeit der Videoüberwachung mit einer „gefühlten Unsicherheit“ der Mandantschaft begründet. Der TLfDI wird im nächsten Berichtszeitraum in einem Anordnungsbescheid die verantwortliche Stelle auffordern, eine Liste der zum Einsatz kommenden Kameras sowie die dazugehörigen Screenshots des Aufnahmebereiches zu übermitteln, um dann geeignete Maßnahmen anzuordnen, damit datenschutzgerechte Zustände wiederhergestellt werden. Seine Forderungen kann der TLfDI dann mithilfe von Zwangsmitteln durchsetzen. Eine Vorort-

kontrolle bot sich in diesem Fall nicht an, da die übermittelten Fotos einen guten Einblick in die Videoüberwachung ermöglichten. Für eine rechtswirksame Anordnung müssen aber die zum Einsatz kommenden Kameras zweifelsfrei benannt werden können. Außerdem besteht die Möglichkeit, ein Bußgeldverfahren einzuleiten, denn nach § 43 Abs. 1 Nr. 10 BDSG handelt ordnungswidrig, wer entgegen § 38 Abs. 3 Satz 1 BDSG eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt.

Die Sachverhaltsaufklärung des TLfDI gestaltet sich mitunter schwierig. Die vom TLfDI geforderten Angaben werden teilweise nur unvollständig gemacht, sodass eine abschließende Beurteilung nicht möglich ist. Kommt eine verantwortliche Stelle den Bitten des TLfDI auf Auskunft nicht nach, wird der TLfDI einen Anordnungsbescheid nach § 38 Abs. 5 Satz 1 BDSG erlassen und seine Forderung nötigenfalls mit Zwangsgeld durchsetzen. Auch die Einleitung eines Bußgeldverfahrens ist nach § 43 Abs. 1 Nr. 10 BDSG möglich.

4.68 In der Spielhalle geht nicht alles – Videogaga 66

Gerade in Spielhallen ist der Einsatz von Videokameras sehr verbreitet. Dort kommt es erfahrungsgemäß häufiger zu Überfällen und es besteht die Gefahr, dass Spielautomaten manipuliert werden. Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) liegen einige Beschwerden zu Spielhallen vor. Nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Betreiber von Spielhallen verweisen als Erlaubnisnorm für die Videoüberwachung oft auf § 6 der Unfallverhütungsvorschriften (UVV) „Spielhallen, Spielkasinos und Automatensäle von Spielbanken“. Nach § 6 Abs. 2 der UVV müssen optische Raumüberwachungsanlagen in Spielhallen so installiert sein, dass wesentliche Phasen eines Überfalles optisch wiedergegeben werden können. Eine derartige Vorschrift, die die Berufsgenossenschaften als Träger der Unfallversicherung erlassen, stellt keine Rechtsgrundlage im Sinne von § 4 Abs. 1 BDSG dar. Sie ist allerdings im Rahmen der rechtlichen Bewertung zu berücksichtigen. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welcher die Videoüberwachung

von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Soll die Videoüberwachung wie im Fall von Spielhallen dazu eingesetzt werden, vor Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. In bestimmten Fällen kann auch eine abstrakte Gefährdungslage ausreichend sein, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die wertvolle Ware verkaufen oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind. Dies ist nach Auffassung des TLfDI bei einer Spielhalle der Fall.
Vor dem Einsatz eines Videoüberwachungssystems ist trotzdem zu überprüfen, ob es im Einzelfall tatsächlich für den festgelegten Zweck geeignet und erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann. Vor der Installation einer Videoüberwachungsanlage muss man sich deshalb mit zumutbaren alternativen Methoden auseinandersetzen, die in das Persönlichkeitsrecht des Einzelnen weniger eingreifen. Vor Inbetriebnahme einer Kameraanlage muss überprüft werden, an welchen Orten und zu welchen Zeiten eine Überwachung unbedingt notwendig ist. Häufig kann eine Überwachung in den Nachtstunden oder außerhalb der Geschäftszeiten ausreichen. Im Rahmen der Erforderlichkeit ist ferner zu untersuchen, ob eine reine Beobachtung im Wege des Live-Monitorings ausreicht oder ob es zum Erreichen des Überwachungszwecks einer (regelmäßig eingriffsintensiveren) Aufzeichnung bedarf. Die Regelung des § 3 Abs. 2 Satz 2 Thüringer Spielhallengesetz rechtfertigt nur ein Monitoring. Danach muss die Aufsicht des Unternehmens von ihrem regelmäßigen Aufenthaltsort aus, auch unter Zuhilfenahme technischer Einrichtungen, alle Spielgeräte einsehen und Spieler beobachten können.

Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung des berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.
Aufgrund dessen kann aus Sicht des TLfDI eine Videoüberwachung nur in den Bereichen gerechtfertigt sein, in denen eine erhöhte Gefahr der Kriminalität besteht. Dies betrifft die Bereiche mit Spielautomaten, bei denen die Gefahr des Aufbruchs oder der Manipulation besteht.
Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden. Denkbar sind offene Überwachungsmaßnahmen danach jedoch insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten in besonders gefahrträchtigen Arbeitsbereichen. Dies ist beispielsweise im Kassenbereich der Fall. Jedoch ist in diesem Zusammenhang der Erfassungsbereich auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte soweit wie möglich auszublenden.
Vor dem Einsatz der Videoüberwachung sind einige Maßnahmen nach dem BDSG durchzuführen. Es ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen. Vor der Inbetriebnahme einer Videoüberwachung ist eine Vorabkontrolle nach § 4d Abs. 5 BDSG erforderlich, wenn bei dem Einsatz der Videotechnik von besonderen Risiken für die Rechte und Freiheiten der Betroffenen auszugehen ist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Dies ist in den meisten Spielhallen der Fall. Der betriebliche Datenschutzbeauftragte (bDSB) hat gemäß § 4d Abs. 6 BDSG die Vorabkontrolle durchzuführen und das Ergebnis sowie die Begründung schriftlich zu dokumentieren. Darüber hinaus ist für Verfahren, die automatisiert Daten verarbeiten, eine Verfahrensübersicht zu erstellen (vergleiche § 4g Abs. 2 und 2a BDSG). Eine Videoüberwachung ist jedenfalls dann, wenn sie mittels digitaler Technik erfolgt, als automatisierte Verarbeitung zu qualifizieren. Welche Angaben in diese Übersicht aufgenommen werden müssen, zählt § 4e Satz 1 BDSG verbindlich und abschließend auf. Die Verfahrensübersicht ist von der verantwortlichen Stelle zu erstellen und dem betrieblichen Datenschutzbeauftragten zur

Verfügung zu stellen. In jedem Fall bedarf es nach § 9 BDSG schriftlicher Festlegungen dazu, unter welcher Voraussetzung durch wen Einsicht in die Aufnahmen genommen werden darf und auf welche Weise dies zu protokollieren ist. Entsprechende schriftliche Festlegungen verlangt der TLfDI von den kontrollierten Stellen. Es wird immer im Einzelfall geprüft, ob der Einsatz aller Kameras tatsächlich erforderlich ist.

Auch wenn in Spielhallen eine größere Gefahr von Überfällen und Manipulationen an den Spielgeräten besteht, kann eine Videoüberwachung zulässigerweise nur betrieben werden, wenn die Voraussetzungen des § 6b BDSG eingehalten werden. Zwar hat ein Spielhallenbetreiber grundsätzlich ein berechtigtes Interesse an der Videoüberwachung. Er muss trotzdem in jedem Einzelfall die Erforderlichkeit des Kameraeinsatzes prüfen und die schutzwürdigen Interessen der Betroffenen (Kunden, Mitarbeiter) berücksichtigen.

4.69 Türspion – Videogaga 67

Wie schon so oft in diesem Tätigkeitsbericht dargestellt, hat sich im Berichtszeitraum mal wieder eine Privatperson mit einer Videokamera am Fenster im zweiten Obergeschoss ausgerüstet. Dies haben im Rahmen des täglichen Streifendienstes Vollzugsdienstkräfte der Abteilung Stadtordnungsdienst und Bußgeldangelegenheiten eines Bürgeramtes in Thüringen festgestellt. Daraufhin wurde dieser Vorgang dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Prüfung übergeben.
Der TLfDI schrieb den Betreiber in einem umfassenden Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) mit der Bitte um Stellungnahme zu der streitgegenständlichen Kamera an. Dieser teilte dem TLfDI mit, dass er mit der Kamera die Haustür und sein davor parkendes Auto überwacht habe. Denn sein Auto sei in der Vergangenheit schon mehrfach angefahren und beschädigt worden.
Um das Ergebnis vorwegzunehmen: Der Betreiber zeigte sich einsichtig und teilte dem TLfDI mit, dass er die Kamera entfernt habe. Das Verfahren konnte abgeschlossen werden.
Ganz allgemein lässt sich jedoch sagen, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist,

soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Eine Einwilligung kommt bei Videoüberwachung in der Regel nicht in Betracht, da sich der Kreis der Betroffenen oftmals nicht eingrenzen lässt. Daher bedarf es zur Rechtmäßigkeit der Durchführung der Videoüberwachung einer gesetzlichen Grundlage. Als Erlaubnisnorm kommt ausschließlich § 6b BDSG in Betracht, da es sich bei dem Hauseingangsbereich sowie der Straße um öffentlich zugängliche Räume handelte. Die Überwachung solcher Bereiche ist nur im Rahmen einer Erforderlichkeit des abschließenden Zweckkatalogs des § 6b Abs. 1 Nr. 1 bis 3 BDSG zulässig. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit. Selbst dann dürfen aber keine Anhaltspunkte dafür gegeben sein, dass schutzwürdige Interessen Betroffener die des Kamerabetreibers überwiegen. Dies ist oftmals der Fall und hat die Unzulässigkeit der Überwachung zur Folge.

In der Regel verstößt das Ausrichten einer Videokamera auf eine öffentliche Straße oder einen öffentlichen Fußweg gegen das Datenschutzrecht. Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen.

4.70 Der Stein ist mein – Videogaga 68 – Kamera im Vorgarten

Zu dem Thema, inwieweit eine Kamera im Vorgarten eines eingezäunten Hauses zulässig sein könnte, erreichte im Berichtszeitraum den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage eines Bürgers. Der Bürger teilte dem TLfDI mit, das unbekannte Personen in den letzten fünf Jahren ihm siebenmal seine Natursteinpfeiler, was er auch an Hand entsprechender Fotografien nachweisen konnte, zerstört hätten.

Hierbei handelte es sich nicht um Zerstörungen, die im Vorübergehen vollbracht wurden, sondern um solche, die nur mit erhöhter Gewalteinwirkung bewirkt werden konnten. Der Bürger informierte nach jeder Zerstörung die Polizei und brachte die entsprechenden Sachverhalte zur Anzeige. Daher konnte der Bürger dem TLfDI auch entsprechende Tagebuchnummern der Thüringer Polizei vorlegen.
Um das Ergebnis vorwegzunehmen: Im hiesigen Fall erachtete der TLfDI die geplante Kamera für datenschutzrechtlich zulässig. Bei einer Videoüberwachung, so auch bei der von dem Bürger im Vorgarten geplanten, handelt es sich immer um einen Umgang mit personenbezogenen Daten. Unter einen solchen Umgang versteht der Gesetzgeber das Erheben, Nutzen und Verarbeiten von personenbezogenen Daten. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Es verbleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die ihnen die Videoüberwachung erlaubt, es sei denn, es handelt sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar, vergleiche § 1 Abs. 2 Nr. 3 BDSG.
Aufgrund der von dem Bürger geschilderten und mittels Fotografien dokumentierten Beschädigungen seines Zaunes, war es für den angedachten Zweck der Kamera im umzäunten Vorgarten notwendig, einen kleinen Teil der außerhalb des Grundstückes liegenden Fläche mit zu überwachen. Dieser außerhalb des Grundstücks liegende Bereich wird vom Gesetzgeber als so genannter öffentlich zugänglicher Raum bezeichnet, da zu diesem ein nicht näher bestimmbarer Personenkreis Zugang hat. Die Beobachtung und Aufzeichnung dieses Bereiches ist nur unter der Maßgabe der vom Gesetzgeber getroffenen Regelung des § 6b BDSG zulässig. Danach ist das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, soweit sie zur Wahrnehmung des Hausrechts (Nr. 2) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Beobachtung war in diesem Fall zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich. Ziel der geplanten Videoüberwachung war, entwe-

der die Aufklärung der regelmäßig stattgefundenen Zerstörung der Natursteinpfeiler oder die Verhinderung solcher Zerstörungen durch die abschreckende Wirkung der Videoüberwachungsanlage. In diesem Zusammenhang ist aber zu betonen, dass eine reine Aufzeichnung für präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Dies ist nur bei einem Monitoring gegeben, da dann der Betreiber unmittelbar eingreifen kann. Das bedeutet, dass eine Videoaufzeichnung zur Verhinderung von Straftaten oder Unfällen nicht geeignet ist.
Im vorliegenden Fall stellte die Aufklärung der regelmäßig stattgefundenen Zerstörung der Natursteinpfeiler ein berechtigtes Interesse dar, dessen Zweck konkret vom Bürger festgelegt wurde. Die geplante Videoüberwachungsanlage war daher geeignet, den von dem Bürger genannten Zweck zu erreichen und es war kein Mittel ersichtlich, welches bei gleicher Zumutbarkeit weniger stark in die Rechte Dritter eingegriffen hätte.
Im Ergebnis konnte der TLfDI auch nicht davon ausgehen, dass nach § 6b Abs. 1 BDSG schutzwürdige Interessen der Betroffenen überwogen hätten. Auch lässt die Rechtsprechung (vergleiche AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter mit aufgenommen wird. Aus den von dem Bürger übergebenen Luftaufnahmen ergab sich, dass lediglich ein nicht offensichtlich zum Betreten gedachter Grasstreifen, der zwischen dem Grundstück und dem angrenzenden Fußweg verlief, von der geplanten Videokamera mit erfasst werden sollte. Der Ein-Meter-Raum würde somit nach Feststellung des TLfDI auch nicht überschritten werden.

Die Rechtmäßigkeit einer Videoüberwachung öffentlich zugänglicher Räume, die Private zum Schutz ihres Eigentums vornehmen, bestimmt sich nach § 6b BDSG. Zulässig kann das Aufstellen einer Kamera im Vorgarten eines eingezäunten Grundstückes mit Ausrichtung auf den Gartenzaun sein, wenn es zuvor zu wiederholtem Zerstörungen und ähnlichen Vorkommnissen an dem Gartenzaun gekommen ist.

4.71 Kameraattrappe blickt in den öffentlichen Verkehrsraum – Videogaga 69

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Ereignismeldung der zuständigen Polizeiinspektion zu einer Videoüberwachungsanlage. Diese wurde im Rahmen eines Ermittlungsauftrages zur Aufklärung von Straftaten festgestellt. Von den Polizeibeamten konnte allerdings nicht geprüft werden, ob es sich um eine funktionstüchtige Kamera oder um eine Attrappe handelte. Jedenfalls war die Kamera auf den öffentlichen Raum (Gehweg und Bundesstraße) gerichtet. Im Laufe des Bearbeitungsverfahrens stellte sich heraus, dass die angezeigte Videokamera zum Schutz des Eigentums des Kamerabetreibers angebracht wurde. Er teilte dem TLfDI mit, dass wiederholt Einbruchsversuche, Diebstähle und Fensterbeschädigungen verübt worden wären. Auch handele es sich bei der Videokamera um eine Attrappe.
Mit dem Einsatz von Kameraattrappen kann auch ein Eingriff in das allgemeine Persönlichkeitsrecht verbunden sein, denn die Kameraattrappe soll bei den Betroffenen die Vorstellung einer funktionsfähigen Anlage erzeugen, um sie von einem unerwünschten Verhalten abzuhalten. Gerade von Kameraattrappen, die aus objektiver Sicht den Anschein der Echtheit erwecken, geht derselbe Anpassungs- und Überwachungsdruck wie von funktionstüchtigen Kameras aus. Der Kamerabetreiber stützte sich darauf, dass das Glas der Kameraattrappe erkennbar geschwärzt sei und dadurch diese nicht den Anschein der Echtheit erwecke. Dieses war vorliegend nicht maßgeblich, denn nach heutigem Stand der Technik gibt es bereits getönte Folien, auch solche könnten auf das Glas einer echten Kamera gezogen werden. Fraglich erschien auch, wie das bloße Auge eindeutig ein geschwärztes Glas der Kamera, welche sich nach Aussage des Kamerabetreibers in 6 Meter Höhe befand, erkennen können soll.
Die Aufstellung einer solchen Attrappe stellte für den Betroffenen die dauernde Androhung einer Videoüberwachung dar und führte bei diesem zu einer psychischen Zwangswirkung. Die betroffene Person sah sich damit in jedem Fall einer Kontrollmöglichkeit ausgesetzt. Daher war der Kontrolldruck nicht anders zu beurteilen als bei einem tatsächlichen Videoeinsatz. Die unbefangene, von Zwangswirkungen freie Kommunikation, Interaktion und Darstellung in der Öffentlich-

keit ist aber Grundbedingung für die freie Entfaltung der Persönlichkeit.
Im Ergebnis wurde die Kameraattrappe vom TLfDI nicht anders behandelt als das funktionierende Modell. Eine Überwachung des öffentlichen Raumes war daher nur unter bestimmten Umständen rechtlich zulässig. Der Kamerabetreiber wurde gebeten, einen umfangreichen Fragenkatalog des TLfDI unter Fristsetzung zu beantworten. Denn nach § 38 Abs. 3 Satz 1 BDSG haben die verantwortlichen Stellen dem TLfDI auf dessen Verlangen die Auskunft zu erteilen. Daraufhin wurde die Kameraattrappe entfernt.

Die Montage einer Kameraattrappe stellt für die Betroffenen eine dauernde Androhung einer Videoüberwachung dar und führt bei diesen zu einem Kontrolldruck. Daher sind Kameraattrappen ebenso nach § 6b BDSG zu bewerten wie funktionstüchtige Modelle.

4.72 Besuch im Blick – Videogaga 70 – Videoüberwachung im Mietshaus

Gerade im unmittelbaren Wohnumfeld nimmt die Videoüberwachung stetig zu. Genau zu diesem Thema erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde. Die Mieterin beschwerte sich über eine Videokamera im Aufzugsvorraum in ihrem Mietshaus. Vor allem, wenn sie Besuch empfing, hätten sich ihre Gäste regelmäßig beobachtet gefühlt. Dies konnte die Mieterin dem TLfDI auch an Hand von Aufnahmen der streitgegenständlichen Kamera glaubhaft machen. Daraufhin schrieb der TLfDI mit einem umfassenden Auskunftsersuchen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) die Wohnungsbaugenossenschaft als Betreiber der Videokamera und damit verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG an. Die Wohnungsbaugenossenschaft teilte dem TLfDI mit, dass keine Videoüberwachung in dem Wohnhaus der Mieterin installiert sei. Diese Auskunft der Wohnungsbaugenossenschaft stand jedoch im Gegensatz zu den dem TLfDI vorliegenden Informationen der Mieterin samt Bildmaterial über die streitgegenständliche Kamera. Deshalb wies der TLfDI die Wohnungsbaugenossenschaft darauf hin, sollte es sich bei der streitgegenständlichen Kamera lediglich um eine Attrappe gehandelt haben, dass Attrappen wegen des gleichen Überwachungsdrucks grundsätzlich nach den gleichen Maßstäben

wie tatsächlich funktionsfähige Kameras zu beurteilen sind (vergleiche Beitrag Nummer 4.27).
Eine Überwachung des Hausflurs in einem Mehrparteienhaus ist nur unter bestimmten Umständen rechtlich zulässig. Insofern ist auch bei Verwendung von Attrappen zu prüfen, ob die datenschutzrechtlichen Vorgaben eingehalten wurden oder nicht. In allen Bereichen, in denen sich danach der echte Kameraeinsatz verbietet, würde somit auch der Einsatz von Kameraattrappen einen Rechtsverstoß bedeuten. Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Es bleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn es handelt sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar, vergleiche § 1 Abs. 2 Nr. 3 BDSG. Die Zulässigkeit der Videoüberwachung in öffentlich zugänglichen Bereichen eines Mehrfamilienhauses oder einer Wohnanlage richtet sich nach § 6b Abs. 1, Abs. 3 BDSG. Beispiele für derartige Bereiche sind etwa Grünflächen und Spielplätze auf dem Gelände, der Eingangsbereich vor der Haustür, der Abstellplatz von Müllcontainern und Fahrradständer außerhalb des Hauses, die außen angebrachten Briefkästen. Zur Wahrung der schutzwürdigen Belange der Mieterinnen und Mieter sind dabei strenge Anforderungen an das Vorliegen der Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG zu stellen. Der § 6b BDSG regelt ausschließlich die Voraussetzungen und Grenzen einer Videoüberwachung in öffentlich zugänglichen Bereichen. Wenn es sich, wie hier, um Räume handelt, die nicht öffentlich zugänglich sind, ist § 6b BDSG nicht anwendbar. Aber auch in diesem Fall sind die von der Videoüberwachung betroffenen Personen in ihrem Persönlichkeitsrecht geschützt. Die Zulässigkeit einer digitalen Videoüberwachung nicht öffentlich zugänglicher Bereiche richtet sich dann nach § 28 Abs. 1 Nr. 2 BDSG. Nicht öffentlich zugängliche Bereiche von Mietshäusern und Wohnanlagen sind zum Beispiel Hausflure, Treppenhäuser, Aufzüge, Waschmaschinen- und Trockenräume sowie Fahrradkeller. Im nicht öffentlich zugänglichen Raum hat die Privatsphäre eine noch höhere Bedeutung als im öffentlich zugänglichen Raum. Gerade hier wissen die Mieter und Mieterinnen, dass sie sich in einem Bereich befinden, zu dem nur eine begrenzte Zahl von Personen Zutritt hat. Der Überwachungsdruck wird hier zumeist noch stärker wahrgenommen als im öffentlich zugänglichen Bereich. Vor allem sind hier von den Über-

wachungsmaßnahmen regelmäßig viele Personen – die Mieterinnen und Mieter und ebenso eine unbestimmte Zahl an Besucherinnen und Besuchern – betroffen. Nach Maßgabe des § 28 Abs. 1 Nr. 2 BDSG dürfen personenbezogene Daten – hier: Bilddaten – zur Wahrnehmung berechtigter Interessen nur dann verarbeitet werden, soweit es erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss einer Videoüberwachung überwiegen. Die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, sind bei deren Erhebung konkret festzulegen. Außerdem hat nach § 4 Abs. 3 BDSG auch hier ein Hinweis auf die Videoüberwachung zu erfolgen (vergleiche Simitis, BDSG Kommentar, § 4, Rn. 45 f.). Nach dieser Norm sind Betroffene von der für die Videoüberwachung verantwortlichen Stelle vor der Erhebung von (Bild-) Daten über die Überwachung und die verantwortliche Stelle zu unterrichten. Eine heimliche Videoüberwachung ist also auch im nicht öffentlich zugänglichen Raum nicht zulässig. Innerhalb eines nicht öffentlich zugänglichen Bereichs kann eine Videoüberwachung zur Wahrnehmung des Hausrechts insbesondere zulässig sein, wenn sie sicherstellen soll, dass technische Einrichtungen wie Fahrstühle, Lastenaufzüge, Lichtschranken etc. störungsfrei funktionieren. Einer personenscharfen Überwachung bedarf es dabei nur, wenn beabsichtigt ist, Täterinnen und Täter, die diese Funktionsfähigkeit manipulieren, gegebenenfalls zu überführen. Dies dient auch der Sicherheit der Benutzerinnen und Benutzer. Allerdings sind auch hier wie stets die schutzwürdigen Interessen der Betroffenen zu beachten.
Auf die erneute Anfrage des TLfDI antwortete die Wohnungsbaugenossenschaft abermals, dass weder eine Kamera noch eine Kameraattrappe in dem Wohnhaus installiert war. Dieser Mitteilung fügte die Wohnungsbaugenossenschaft auch Aufnahmen bei, die das Nicht-Vorhandensein einer Kamera bestätigten. Da sich der Sachverhalt nachträglich aufgrund der gegensätzlichen Darstellung der Mieterin und der Wohnungsbaugenossenschaft für den TLfDI nur schwer aufklären ließ und die Kamera nun offensichtlich nicht mehr vorhanden war, konnte das Verfahren abgeschlossen werden.

Die Zulässigkeit einer digitalen Videoüberwachung nicht öffentlich zugänglicher Bereiche in Mietshäusern und Wohnanlagen, wie Hausflure, Treppenhäuser, Aufzüge, Waschmaschinen- und Trockenräume sowie Fahrradkeller richtet sich nach § 28 Abs. 1 Nr. 2 BDSG.

Danach dürfen personenbezogene Daten – Videoaufnahmen – zur Wahrnehmung berechtigter Interessen nur dann verarbeitet werden, soweit es erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss einer Videoüberwachung überwiegen.

4.73 Schnitzel und Spitzel – Videogaga 71 – Videoüberwachung im Restaurant

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt in einem weiteren Fall Kenntnis von einer Videoüberwachung in einem Restaurant. Dabei berichtete ein Bürger, der Gast in dem Lokal gewesen war, von mindestens zwei festinstallierten Kameras in der Gaststube, deren Ausrichtung vermuten ließ, dass hiermit sowohl Arbeitsbereiche als auch Sitzplätze erfasst wurden. Die Beobachtung war gemäß § 6b Bundesdatenschutzgesetz (BDSG) zu beurteilen. Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG zur eingesetzten Videoüberwachung an die Geschäftsleitung des Restaurants. Da keine fristgerechte Auskunft an den TLfDI erfolgte, wurde ein bereits in dem Auskunftsersuchen angedrohtes Zwangsgeld festgesetzt und die notwendigen Unterlagen zur Vollstreckung des Zwangsgeldes an das zuständige Finanzamt übersandt. Zwischenzeitlich bekam der TLfDI von der Geschäftsführung des Restaurants eine Mitteilung, wonach man bereits rechtzeitig auf das Auskunftsverlangen des TLfDI geantwortet habe. Dieses Schreiben sei nach Vermutung des Geschäftsführers des Restaurants wohl auf dem Postweg verloren gegangen. Es wurde deshalb als Anlage nochmals beigefügt. Hieraus war zu entnehmen, dass die Videoanlage von einem ehemaligen Geschäftsführer installiert worden sein soll und nicht funktionstüchtig sei. Dem TLfDI wurde zugesagt, die Kameras kurzfristig aus dem Restaurant zu entfernen. Von den hierfür ergriffenen Maßnahmen überzeugte sich der TLfDI bei einer Vorortkontrolle im Restaurant. Daraufhin war die Vollstreckungsmaßnahme gegen die Gaststätte einzustellen, da die mit dem angedrohten und festgesetzten Zwangsgeld durchzusetzende Handlung erfüllt wurde. Abschließend wurde die Geschäftsführung des Lokals über die Beendigung des Verwaltungsverfahrens unterrichtet.

Beantwortet eine nicht-öffentliche Stelle ein Auskunftsverlangen des TLfDI nach § 38 Abs. 3 BDSG nicht oder nicht vollständig, so kann der TLfDI ein Zwangsgeld gegen die Stelle festsetzen. Die Zwangsgeldzahlung und deren Zwangsvollstreckung kann abgewendet werden, wenn die verlangten Auskünfte noch erteilt werden.

4.74 Überwachungskunst – Videogaga 72 – Video in der Kunstausstellung

Im Berichtszeitraum meldete sich ein besorgter Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er teilte dem TLfDI mit, dass er bei einem Besuch einer Kunstausstellung eine Videoüberwachung in den Ausstellungsräumlichkeiten festgestellt habe. Als Besucher der Ausstellung sei man beim Betreten der Räumlichkeiten sofort in den Erfassungsbereich gelangt und darauf nicht hingewiesen worden. Erst bei einem erneuten Besuch der Kunstausstellung konnte der Bürger ein Schild, das auf eine „elektronische Überwachung“ hinwies, feststellen. Nachdem der Bürger von seinem Recht Gebrauch machte und das für die Videoüberwachung verantwortliche Unternehmen auf die Kamera ansprach, versicherte dieses, dass die Kamera nicht während der Öffnungszeiten der Kunstausstellung in Betrieb sei.
Daraufhin kontaktierte der TLfDI das Unternehmen mit der Bitte um Stellungnahme zu der betriebenen Videoüberwachungsanlage in der Kunstausstellung. Dieses berichtete dem TLfDI, dass die monierte Kamera inzwischen abgebaut sei und es sich außerdem auch nicht um eine funktionstüchtige Kamera, sondern um eine Attrappe gehandelt habe.
Wie schon unter Nummer 4.27 ausführlich dargestellt, unterscheiden sich solche Attrappen in der datenschutzrechtlichen Prüfung kaum von richtigen Kameras. Dies liegt vor allem daran, dass es subjektiv für den Betroffenen keinerlei Unterschiede macht, ob eine Kamera in Betrieb bzw. ausgeschaltet ist, oder ob es sich um eine Attrappe handelt. Denn der Zustand einer solchen Videoüberwachung ist von außen für die Betroffenen nicht erkennbar. Im Ergebnis bleibt daher der Überwachungsdruck für die Betroffenen gleich. Genau das führt zu einer Verhaltensveränderung und stellt damit einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Daher sind auch Attrappen nur zulässig, wenn auch eine funktionstüchtige Kamera zulässig wäre. Die Zulässigkeit bestimmt sich bei der Videoüberwachung von öf-

fentlich zugänglichen Räumen, wie hier bei einer Kunstausstellung, in der Regel nach § 6b Bundesdatenschutzgesetz (BDSG). Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit es zur Wahrnehmung des Hausrechts (Nr. 2) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr.3) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Mit der Mitteilung allerdings, dass das Unternehmen die Kameraattrappe entfernt habe, konnte das Verwaltungsverfahren vom TLfDI abgeschlossen werden.

Wegen des gleichen Überwachungsdrucks wie bei einer funktionstüchtigen Kamera sind auch Attrappen nur zulässig, wenn eine funktionstüchtige Kamera zulässig wäre. Dies bestimmt sich bei Videoüberwachung von öffentlich zugänglichen Räumen, wie bei Kunstaustellungen, in der Regel nach § 6b Bundesdatenschutzgesetz (BDSG).

4.75 Bitte um Beobachtung – Videogaga 73 – Videoüberwachung im Aufzug

Der Thüringer Landesbeauftrage für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von Bewohnern zweier benachbarter Wohnhochhäuser aufgefordert, sich für die erneute Inbetriebnahme einer Videokamera in den Aufzügen der beiden Häuser einzusetzen. Diese Bitte wurde in Form einer Petition mit beigefügten Unterschriftenlisten eingereicht. Begründet wurde das mit einem Überfall, der sich nach Darstellung eines Presseartikels in einer anderen Wohnanlage des Stadtgebietes offenbar ereignet hatte. Den Bewohnern wurde mitgeteilt, dass die Verantwortung für die Zulässigkeit einer Videoüberwachung in dem Haus die Wohnungsgesellschaft als Vermieterin trage. Die Wohnungsgesellschaft hat aber die gesetzlichen Bestimmungen zu beachten, unter welchen Umständen die Beobachtung mit Videokameras von bestimmten Bereichen des Wohnhauses zulässig ist. Kameras sollten nach den Wünschen der Mieter im Fahrstuhl, im Treppenhaus und im Flur installiert werden. Der TLfDI klärte die Mieter über die Rechtslage auf: Bei den betroffenen Bereichen handelt es sich nicht um öffentlich zugänglichen Raum. Denn das Gebäude dürfen grundsätzlich nur die Mieter und

weitere hierfür autorisierte Personen betreten, nicht aber jeder, der dies beabsichtigt. Somit kommen zur Bewertung des Sachverhalts die speziellen Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Videoüberwachung in § 6b nicht zur Anwendung. Vielmehr erfolgt die Zulässigkeitsprüfung nach den allgemeinen Bestimmungen des § 28 BDSG zur Erhebung und Verarbeitung von personenbezogenen Daten. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten nur zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Wohnungsgesellschaft erforderlich ist. Es darf außerdem kein Grund zur Annahme bestehen, dass das schutzwürdige Interesse von Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Dies ist beispielsweise anzunehmen, wenn Mieter die Unterschriftenliste nicht unterzeichnet haben und sich durch die Kamera in ihrem Recht auf informationelle Selbstbestimmung eingeschränkt sehen. Im Ergebnis standen die berechtigten Interessen der Wohnungsgesellschaft an einer Videoüberwachung im Fahrstuhl des Gebäudes den schutzwürdigen Interessen der Betroffenen gegenüber. Es war somit eine Interessenabwägung vorzunehmen. Die Verhinderung körperlicher Übergriffe auf Nutzer des Fahrstuhls kann ein berechtigtes Interesse des Vermieters darstellen. Allerdings erfolgte der Übergriff, der Ursache für die Einführung der Videoüberwachung war, auf eine Person in einem anderen Haus und lag fast ein Jahr zurück. Für den TLfDI haben sich die Umstände so dargestellt, dass einerseits keine tatsächliche Gefahr, sondern ein Interesse an der Abwehr einer abstrakten Gefahr festzustellen war, andererseits aber ein Interesse von Mietern und ihren Besuchern auf Schutz vor ungerechtfertigter oder unangemessener Beobachtung geltend gemacht werden konnte. Daher ging der TLfDI nach Prüfung aller ihm bekannten Umstände davon aus, dass das schutzwürdige Interesse von Betroffenen, deren Persönlichkeitsrechte durch die Videobeobachtung verletzt wird, überwiegt. Dabei kommt es nicht darauf an, ob es sich um Befürworter oder Gegner der Videoüberwachung oder um völlig ahnungslose Besucher handelt. Dem TLfDI sind darüber hinaus zahlreiche Gerichtsentscheidungen zu ähnlichen Konstellationen der Videoüberwachung in Fahrstühlen bekannt. Den Urteilsbegründungen ist zu entnehmen, dass die Hürden für einen zulässigen Einsatz einer Videoüberwachung in Fahrstühlen hoch sind, da es sich um eine besonders eingriffsstarke Maßnahme handelt. Dies ergibt sich z. B. aus der Raumgröße eines Fahrstuhls, sodass man einer

darin angebrachten Videokamera „Auge in Auge“ gegenübersteht und keinerlei Ausweichmöglichkeiten besitzt.

Der TLfDI prüft u. a. die Zulässigkeit von Videoüberwachungen. Es gehört jedoch nicht zu seinen gesetzlich zugewiesenen Aufgaben, sich aktiv gegenüber einer Stelle für eine Videoüberwachung einzusetzen. Im konkreten Fall wäre eine Videoüberwachung zudem nicht zulässig gewesen.

4.76 Kamera-Detektiv – Videogaga 74

Im Berichtszeitraum bat die Detektei eines Drogeriemarktes den Thüringer Landesbeauftragten für Datenschutz und die Informationsfreiheit (TLfDI) um Beratung im Hinblick auf die Installation einer Videoüberwachungsanlage. Die Frage war, wie dies ohne die Verletzung von Vorschriften des Bundesdatenschutzgesetzes (BDSG) durchgeführt werden könnte. In dem betreffenden Fall waren in der Vergangenheit mehrfach die Fensterscheiben des Auftraggebers der Detektei – ein Drogeriemarkt – eingeschlagen worden. Dieses konnte die Detektei dem TLfDI auch an Hand eingetragener polizeilicher Tagebuchnummern glaubhaft machen. Mithilfe einer Videoüberwachung sollten nun nach Aussage der Detektei mögliche zukünftige Täter identifiziert werden. Dabei ließe es sich aber nicht vermeiden, dass auch ein gewisser Teil des öffentlichen Raumes mit beobachtet werde. Nach Angaben der Detektei sollte der Bereich der Aufzeichnung etwa fünf bis sieben Meter in den öffentlichen Raum hineinreichen. Eine Auswertung sollte nach dem so genannten Black-Box-Prinzip erfolgen, d. h. nur, wenn es tatsächlich zu Vorfällen gekommen ist. Ansonsten sollten die Daten alle 72 Stunden überschrieben werden.
Die Rechtsgrundlage für die von dem Drogeriemarkt angestrebte Beobachtung des öffentlich zugänglichen Raumes ist § 6b Abs. 1 Nr. 3, Abs. 3 BDSG. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Im vorliegenden Fall stellte die Beobachtung von Schaufenstern, die in der Vergangenheit eingeschlagen wurden, ein solches berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3

BDSG dar. Ebenfalls darf diese Beobachtung nur zu konkret festgelegten Zwecken durchgeführt werden. Daher müssen die Zwecke vorab in einem Verfahrensverzeichnis festgelegt werden. Das Verfahrensverzeichnis ist ein Element des deutschen Datenschutzes. Nach § 4d, § 4e BDSG muss jede verantwortliche Stelle, die personenbezogene Daten verarbeitet, den Umgang mit diesen Daten dokumentieren. Gemäß § 4g Abs. 2 S. 1 BDSG ist von der verantwortlichen Stelle eine Übersicht über die in § 4e S. 1 BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen (häufig bezeichnet als "internes Verfahrensverzeichnis"). Soweit im Unternehmen ein Datenschutzbeauftragter ernannt ist, macht dieser gemäß § 4g Abs. 2 S. 2 BDSG Teile dieses "internen Verfahrensverzeichnisses" (konkret die Angaben nach § 4e S. 1 Nr. 1 bis 8 BDSG) auf Antrag jedermann in geeigneter Weise verfügbar. Man spricht insoweit häufig vom "öffentlichen Verfahrensverzeichnis". Sofern ein Datenschutzbeauftragter nicht bestellt ist, obliegt diese Verpflichtung der verantwortlichen Stelle.
Diese geplante Videobeobachtung ist gemäß § 6b Abs. 1 BDSG allerdings nur soweit zulässig, wie sie für das Erreichen der o. g. Zwecke erforderlich ist. Daher ist jede Beobachtung öffentlich zugänglicher Bereiche, die über diesen Zweck hinausgeht, nicht erforderlich und damit unzulässig. Ebenfalls ist jede Beobachtung dann unzulässig, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen. Je mehr (unbeteiligte) Betroffene in den Aufnahmebereich der Videoüberwachung geraten, desto wahrscheinlicher liegen Anhaltspunkte für das Überwiegen deren schutzwürdiger Interessen vor. Je weiter also der überwachte Bereich ausgedehnt ist, desto eher liegen solche Anhaltspunkte vor. Zwar lässt die Rechtsprechung (vergleiche AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter mit aufgenommen wird, bei fünf bis sieben Metern, wie im vorliegenden Fall, ist die Beobachtung aber in jedem Fall unzulässig.
Des Weiteren wies der TLfDI noch den Drogeriemarkt darauf hin, dass auf die Videoüberwachung nach § 6b Abs. 2 BDSG hinzuweisen ist. Denn eine verdeckte Videoüberwachung von öffentlich zugänglichen Bereichen ist unzulässig. Soweit der Drogeriemarkt das Speichern der Videoaufnahmen vorsieht, richtet sich dies nach § 6b Abs. 3. Danach ist die Verarbeitung oder Nutzung von personenbe-

zogenen Daten zulässig, wenn diese zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Speicherung der personenbezogenen Daten ist daher nur für die Dauer, in der üblicherweise ein Vorfall entdeckt wird, erforderlich. Dies ist im Hinblick auf die Öffnungszeiten von Geschäften differenziert zu betrachten. Zu Geschäftszeiten wird das Einschlagen eines Fensters quasi sofort entdeckt. Zur Zweckerreichung ist somit eine Aufzeichnungsdauer von nicht mehr als einer Stunde mehr als ausreichend. Ebenfalls ist bei einer so kurzen Aufzeichnungsdauer auch bei regelmäßigem Publikumsverkehr nicht davon auszugehen, dass schutzwürdige Interessen Betroffener solche der verantwortlichen Stelle überwiegen. Gleiches gilt für die Zeiten außerhalb der Geschäftszeiten. Hier ist eine Aufzeichnung von 24 Stunden ausreichend. Lediglich über das Wochenende kann die Aufzeichnungsdauer auf 72 Stunden erhöht werden, um Überwachungslücken zu vermeiden.
Letztlich ist von der verantwortlichen Stelle oder von dem betrieblichen Datenschutzbeauftragten in eigener Verantwortung in regelmäßigen Zeitintervallen zu prüfen, ob sich die Interessenlagen verschieben und so Anhaltspunkte vorliegen, dass schutzwürdige Interessen Betroffener überwiegen oder die Videoüberwachungsanlage insgesamt nicht mehr erforderlich ist. Kommt es beispielsweise über einen längeren Zeitraum zu keinerlei Vorfällen, können schutzwürdige Interessen Betroffener überwiegen. Werden Täter gefasst, insbesondere die, die für die Vorfälle in der Vergangenheit verantwortlich sind, kann die Erforderlichkeit der Anlage entfallen.
Im Ergebnis teilte der TLfDI der Detektei des Drogeriemarktes mit, dass das beschriebene Vorhaben momentan als nicht mit dem BDSG vereinbar erscheint.

In großen Supermärkten, Einkaufszentren und den vielen weiteren Geschäften gehören Videokameras schon fast zum gewohnten Bild. Das bedeutet allerdings nicht, dass jede der praktizierten Videoüberwachungen datenschutzrechtlich zulässig ist. Der Gesetzgeber hat den Einsatz von Videotechnik auch für diese Bereiche nicht generell erlaubt, sondern denselben Anforderungen des § 6b BDSG wie jede andere Videoüberwachung öffentlich zugänglicher Räume durch Private unterworfen. Es obliegt daher den Verantwortlichen, auch hier die Zulässigkeit der Videoüberwachung – gegebenenfalls

im Rahmen eines Gesamtkonzepts – einzelfallbezogen zu prüfen und zu begründen.

4.77 Meldepflicht für Videoanlagen

Mit Urteil vom 11. Dezember 2014 hat der Gerichtshof der Europäischen Union in Luxemburg (EuGH) entschieden, dass die EU-Datenschutzrichtlinie auch auf privat betriebene Videoüberwachungen Anwendung findet, wenn damit öffentlicher Raum, wie zum Beispiel Gehwege und Straßen, überwacht wird. Darüber hinaus hat der EuGH bestätigt, dass eine Speicherung der mittels einer Videoüberwachung gewonnenen Bilddaten als automatisierte Verarbeitung im Sinne der EU-Datenschutzrichtlinie gilt. In § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) werden die verbindlichen Regelungen der „Pflicht zur Meldung bei der Kontrollstelle“ (Art. 18) und der „Vorabkontrolle“ (Art. 20) der EU-Datenschutzrichtlinie umgesetzt. Danach sind alle Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, vor ihrer Inbetriebnahme von nichtöffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde, sprich dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), zu melden. Ein Verfahren fasst alle Verarbeitungen zusammen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmungen realisiert werden sollen. Daher kann ein Verfahren eine Vielzahl von Datenverarbeitungsvorgängen umfassen, z. B. solche zur Personaldatenverarbeitung, für Abrechnungen oder für Marketingzwecke. Auch die automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Aufnahmen im Rahmen einer Videoüberwachung löst eine Meldepflicht für diese Verfahren aus. Die Meldung ist so zu gestalten, dass überprüft werden kann, ob die gemeldeten Verfahren mit den Regeln des BDSG vereinbar sind. Dies gilt insbesondere für den Zweck der beinhalteten Verarbeitungen. Verfahren automatisierter Verarbeitungen, in denen personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (§ 29 BDSG, z. B. Tätigkeiten von Auskunfteien, Adresshandel) oder zum Zweck der anonymisierten Übermittlung (§ 30 BDSG, z. B. Markt- u. Meinungsforschung) gespeichert werden, unterfallen ohne Ausnahme der Meldepflicht (§ 4d Abs. 4 BDSG).

Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz (DSB) bestellt hat (§ 4d Abs. 2

BDSG). Bestimmte verantwortliche Stellen müssen immer einen DSB bestellen und sind, sobald sie der Pflicht zur Bestellung nachgekommen sind, von der Meldepflicht befreit. Eine Pflicht zur Bestellung eines DSB besteht, wenn eine Stelle mit mehr als neun Personen personenbezogene Daten automatisiert erhebt, verarbeitet oder nutzt oder in der Regel mit mindestens zwanzig Personen personenbezogene Daten erhebt, verarbeitet oder nutzt (manuelle Verarbeitung). Weiterhin besteht eine Pflicht zur Bestellung eines DSB, wenn die verantwortliche Stelle automatisierte Verarbeitungen vornimmt, die einer Vorabkontrolle gemäß § 4d Abs. 5 BDSG unterliegen.
Sollte nach Vorgenanntem keine Pflicht zur Bestellung eines DSB bestehen, können verantwortliche Stellen freiwillig einen DSB bestellen und sind dann ebenfalls von der Meldepflicht befreit, vergleiche § 4d Abs. 2 BDSG. Die Bestellung muss dann aber zum Zeitpunkt der Meldepflicht bereits erfolgt sein.
Weitere Informationen können auf der Homepage des TLfDI unter der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ entnommen werden (https://www.tlfdi.de/tlfdi/themen/orientierungshilfen/). Der TLfDI appellierte daher über die Industrie- und Handelskammern (IHK) und Handwerkskammern in Thüringen an die Mitgliedsunternehmen, eine beabsichtigte oder durchgeführte Videoüberwachung zu melden, sofern kein Datenschutzbeauftragter bestellt ist. Auf die vom TLfDI entwickelten Formblätter rund um die Meldepflicht nach § 4d BDSG (https://www.tlfdi.de/tlfdi/themen/unternehmen/) wurde hingewiesen.
Der TLfDI wies nochmals ausdrücklich darauf hin, dass, wer der vorgenannten Meldepflicht nicht nachkommt, nach § 43 Abs. 1 Nr. 1 BDSG eine Ordnungswidrigkeit begeht, die mit einer Geldbuße von bis zu 50.000 Euro geahndet werden kann.

Nach § 4d Abs. 1 BDSG sind Verfahren automatisierter Verarbeitungen – also auch Videoüberwachungsanlagen – vor der Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen grundsätzlich

der zuständigen Aufsichtsbehörde, sprich dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), zu melden. Auch die digitale Videoaufzeichnung stellt eine automatisierte Datenverarbeitung in diesem Sinne dar (vergleiche: Urteil des Gerichtshofs der Europäischen Union in Luxemburg (EuGH) vom 11. Dezember 2014 Rn. 25 sowie die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, dort unter Nummer 2.2.1).

4.78 Kamera versus Concierge – Videogaga 75

Wie würden Sie sich fühlen, wenn Sie als Mieter oder Mieterin einer Wohnung in einem Wohnblock abends von der Arbeit nach Hause kommen und im Conciergebereich nun kein Concierge mehr sitzt, sondern eine Videokamera mit Ausrichtung auf den Eingangsbereich installiert ist? Genau mit solch einem Fall befasste sich der Thüringer Landebeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI). Der Mieter teilte dem TLfDI mit, dass zum Zeitpunkt seines Einzugs der Wohnblock „rund um die Uhr“ mit einem Concierge-Dienst ausgestattet gewesen sei. Gerade dieser Umstand habe ihn als Mieter nicht gestört, denn die als Concierge eingesetzten Mitarbeiter hätten regelmäßig in zeitlichen Abständen gewechselt, sodass kein Eindruck der generellen Beobachtung vermittelt wurde. Mit Einführung des Mindestlohnes für die Berufsgruppe „Sicherheit“ informierte die Wohnungsbaugenossenschaft in einem Rundschreiben alle Mieter und Mieterinnen, dass nun aufgrund der finanziellen Mehrbelastung der Einsatzzeitraum des Concierge zeitlich eingeschränkt werden müsste. Daraufhin erfolgte eine Verkürzung der Besetzungszeiten des Concierge auf 06:00–22:00 Uhr, und die Wohnungsbaugenossenschaft installierte eine Videoüberwachungsanlage in der Conciergeloge sowie weitere drei Kameras mit Ausrichtung auch auf die Notfalltüren.
Danach forderte der TLfDI die Wohnungsbaugenossenschaft zur Stellungnahme zur streitgegenständlichen Videoüberwachungsanlage auf. Diese teilte dem TLfDI in einem umfassenden Auskunftsverlangen mit, dass sie die Kameras zur Überwachung der Conciergeloge bei Abwesenheit des Diensthabenden sowie zur Verschlusssicherheit der Notausgänge habe anbringen lassen. Die im Inneren des Wohnblocks angebrachten Kameras würden die Signale dauernd auf einen nur für den Concierge einsehbaren Monitor bei dessen Anwe-

senheit übertragen. Ebenfalls habe man die Bewohner und Gäste des Wohnblocks durch Hinweisschilder auf die Videoüberwachung hingewiesen. Weiterhin legte die Wohnungsbaugenossenschaft dem TLfDI eine Auflistung sämtlicher Vorfälle aus der Vergangenheit mit Schadensart, Datum, Uhrzeit sowie der Schadenssumme vor.
Wie schon ausführlich im Tätigkeitsbericht „Besuch im Blick in Wohnanlagen“ dargestellt, ist zunächst hinsichtlich der einschlägigen Rechtsvorschrift für die Beurteilung der Zulässigkeit von Videoüberwachung zwischen öffentlich zugänglichen Bereichen und nicht öffentlich zugänglichen Bereichen wie Hausfluren, Treppenaufgängen, Aufzügen, Waschräumen und Fahrradkellern zu unterscheiden. Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b Bundesdatenschutzgesetz (BDSG) richtet. In diesen Fällen greift § 28 BDSG, wonach ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, sind bei deren Erhebung konkret festzulegen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit. Weiterhin ist vor dem Einsatz eines Videoüberwachungssystems grundsätzlich zu prüfen, ob es tatsächlich für den festgesetzten Zweck geeignet und erforderlich ist. Die Erforderlichkeit kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen wirtschaftlich oder organisatorisch zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann. Die Wohnungsbaugenossenschaft teilte dem TLfDI mit, dass wegen der für Wohnhochhäuser besonders geltenden brandschutztechnischen Vorschriften die Bewohner das Haus im Notfall ohne Nutzung von Hilfsmitteln verlassen müssen. Somit können die Notfalltüren von innen

immer geöffnet werden, was Fremden und Unbefugten den Zutritt zum Wohngebäude ermöglicht. Gerade diese Notausgänge seien für den Concierge nicht einsehbar und es wären mindestens immer drei Personen erforderlich, um die drei Notausgänge des Gebäudes zu beaufsichtigen. Deshalb sei nach Auskunft der Wohnungsbaugenossenschaft eine Videoüberwachung dieser Notfalltüren geboten. Vor allem in der Vergangenheit habe es mehrfach solche Vorfälle des unberechtigten Betretens gegeben. Weiterhin führte die Wohnungsbaugenossenschaft aus, dass sie die Kameras installiert habe, um Beweise für die Verfolgung von möglichen Straftaten zu erheben. In diesem Zusammenhang ist aber zu erwähnen, dass eine Aufzeichnung für präventive Zwecke nicht geeignet ist, wenn keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. das Sicherheitspersonal eingreifen kann. Die Strafverfolgung ist zudem Aufgabe der Strafverfolgungsbehörden. Diese haben eigene Ermächtigungsgrundlagen für das Erheben von personenbezogenen Daten. Vorliegend sei die Videoüberwachungsanlage nach Auskunft der Wohnungsbaugenossenschaft gerade dazu notwendig, die Conciergeloge bei Abwesenheit zu überwachen. Ein direktes Eingreifen des Concierge ist daher gerade nicht gegeben. Nach derzeitiger Aktenlage ist die Videoaufzeichnung der Wohnungsbaugenossenschaft zur Verhinderung von Unfällen und Straftaten nicht geeignet.
Das Verfahren ist bisher noch nicht abgeschlossen. Über den Ausgang wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses stellt einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b Bundesdatenschutzgesetz (BDSG) richtet. In diesen Fällen greift § 28 BDSG.

4.79 Dem Mitbewerber auf der Spur – Videogaga 76 – Kameraattrappe bei Dienstleistungsunternehmen

Im Berichtszeitraum beschwerte sich ein Dienstleistungsunternehmen für Kfz-Kennzeichen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über einen

Mitbewerber. Der Mitbewerber, welcher ebenfalls eine Prägestelle für Kfz-Zeichen betreibt, hat seinen Geschäftssitz direkt neben dem des Beschwerdeführers. Grund der Beschwerde war eine am Schilderwagen des Mitbewerbers angebrachte Videokamera, ausgerichtet auf den Geschäftseingang des Beschwerdeführers sowie auf die direkt angrenzende Zulassungsstelle.
Daraufhin schrieb der TLfDI den Mitbewerber mit der Bitte um Stellungnahme zu der streitgegenständlichen Kamera an. Dieser teilte mit, dass er die Kamera angebracht hatte, weil an der Seite zu dem Beschwerdeführer kein Fenster sei und er dadurch nicht sehen konnte, wenn potentielle Kunden aus der Zulassungsstelle kommen. Da es eine relativ preiswerte Kamera aus dem Internet war, konnte er sie aber leider nicht in Betrieb nehmen. Daher habe es sich lediglich um eine Attrappe gehandelt. Der Mitbewerber wurde vom TLfDI auf die Rechtslage zu Kameraattrappen hingewiesen. Eine für echt gehaltene Attrappe wird von den betroffenen Bürgern ebenso als Grundrechtseingriff empfunden wie eine tatsächlich funktionierende Kamera. Die Aufstellung einer solchen Attrappe stellte für den Betroffenen die dauernde Androhung einer Videoüberwachung dar. Die betroffenen Personen sehen sich damit in jedem Fall einer Kontrollmöglichkeit ausgesetzt. Daher war auch hier der Kontrolldruck nicht anders zu beurteilen als bei einem tatsächlichen Videoeinsatz. Die unbefangene, von Zwangswirkungen freie Kommunikation, Interaktion und Darstellung in der Öffentlichkeit ist aber Grundbedingung für die freie Entfaltung der Persönlichkeit.
Im Ergebnis wurde die Kameraattrappe vom TLfDI nicht anders behandelt als das funktionierende Modell. Eine Überwachung des öffentlichen Raumes war daher nur unter bestimmten Umständen rechtlich zulässig. Der Mitbewerber teilte dem TLfDI mit, dass er die Kameraattrappe entfernt habe. Gleichwohl habe er aber vor, ein Nummernschild mit einer so genannten Rückfahrkamera anzubringen. Aufgrund dieser Kamera könne er dann beobachten, wenn potentielle Kunden kommen. Er fragte dazu den TLfDI nach der Zulässigkeit für die von ihm geplante Installation einer solchen Rückfahrkamera. Mit dem Bundesdatenschutzgesetz ist eine solche Videoüberwachung von Kunden und öffentlich zugänglichen Bereichen nur unter den Voraussetzungen des § 6b Abs. 1 BDSG zulässig. An Hand der übermittelten Bilder konnte der TLfDI feststellen, dass der vorgesehene Aufnahmebereich der Rückfahrkamera sehr weit sein sollte und daher für den von dem Mitbewerber durchgeführten

Zweck nicht gerechtfertigt sein würde. Dem Mitbewerber wurde die Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen“ des Düsseldorfer Kreises (siehe unter https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh-v__-durch-nicht-__ffentliche-stellen.pdf), in der Grundsätze zulässiger Videoüberwachung aufgeführt sind, übermittelt.

Mit der Mitteilung, dass der Mitbewerber die Kameraattrappe entfernt habe, konnte das Verfahren abgeschlossen werden.

Die Montage einer Kameraattrappe stellt für die Betroffenen eine dauernde Androhung einer Videoüberwachung dar und führt bei diesen zu einem Kontrolldruck. Daher sind Kameraattrappen ebenso nach § 6b BDSG zu bewerten wie funktionstüchtige Modelle.

4.80 Beim Verzehr kein Genuss? Die Kamera bringt den Verdruss – Videogaga 77 – Videoüberwachung im Restaurant

Bei einer Kontrolle stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) fest, dass in den Räumen eines Restaurants eine umfangreiche Videoüberwachungsanlage betrieben wurde. Insgesamt konnten zehn Kameras festgestellt werden. Dabei handelte es sich um eine Videoüberwachung im Außenbereich des Restaurants sowie Videoüberwachungen im Innenbereich der Gaststätte. Die Kamera im Außenbereich des Restaurants erfasste ausschließlich die Sitzplätze vor dem Lokal und Teile des angrenzenden Gehweges. In den Gasträumen selbst waren insgesamt sieben Kameras installiert, die wenigstens zum Teil, oft aber ausschließlich auf Sitzplätze ausgerichtet waren. Weiterhin betrieb der Gastronom je eine Kamera im zum Lokal gehörenden Lagerraum sowie in der Küche des Lokals. Des Weiteren wurden alle Aufnahmen auf einen HD-Festplattenrekorder übertragen, welcher sich in der Spülküche des Lokals befindet. Das System ist so aufgebaut gewesen, dass die Live-Bilder und Videoaufzeichnungen über das Internet, insbesondere mit Mobiltelefonen, abgerufen werden konnten.

Nachdem der Betreiber des Restaurants die eingeräumte Möglichkeit, zum Sachverhalt Stellung zu nehmen – die sogenannte Anhörung im Sinne des § 28 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) – nicht wahrgenommen hatte, erließ der TLfDI einen Bescheid unter Anordnung der sofortigen Vollziehung. Danach wurde der Gaststättenbetrieb verpflichtet, die Videoüberwachungsanlagen sowohl im Innenbereich als auch im Außenbereich zu deinstallieren. Als Begründung führte der TLfDI aus, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Es handelt sich also um ein materielles Verbot mit Erlaubnisvorbehalt. Die im vorliegenden Fall betriebenen Kameras erhoben solche personenbezogenen Daten, der ebenfalls betriebene Festplattenrekorder führte die Speicherung und damit Verarbeitung dieser Daten durch.
Der TLfDI stellte fest, dass für alle im Innenbereich des Lokals betriebenen Kameras mit Blick auf die Sitzplätze und Tische sowie der angebrachten Außenkamera mit Blick auf die Sitzplätze und Tische auf den angrenzenden Gehweg keine solche gesetzliche Grundlage für die Datenerhebung gegeben war. Auch eine Einwilligung schied in der vorliegenden Konstellation aus. Diese ist grundsätzlich schriftlich einzuholen, was aufgrund des unbestimmten Kundenkreises eines Restaurants nicht umsetzbar war. Darüber hinaus ist die Einwilligung vor Datenerhebung zu erteilen. Bereits mit Eindringen in den äußeren videoüberwachten Bereich, beispielsweise durch das Lesen der außen angebrachten Speisekarte und schließlich mit Betreten des Restaurants, werden Daten von den Kunden erhoben. Auch konnte nicht ausgeschlossen werden, dass vorbeilaufende Fußgänger von der Außenkamera erfasst werden. Soweit von der hier gegenständlichen Videoüberwachung auch Mitarbeiter betroffen waren, schied eine Einwilligung ebenfalls aus. Eine solche ist im Beschäftigungsverhältnis ohnehin nur unter äußerst engen Voraussetzungen möglich, da in der Regel die für die Einwilligung notwendige Freiwilligkeit fehlt. Freiwilligkeit kann nur dann gegeben sein, wenn dem Arbeitnehmer echte Alternativen zu einer Einwilligung aufgezeigt werden und dieser auch ohne eine solche seinen Arbeitspflichten nachkommen kann. Hier musste der videoüberwachte Bereich zwingend von den einzelnen Mitarbeitern betreten werden, weswegen es von vornhinein an der verlangten Freiwilligkeit mangelte.

Als Erlaubnisnorm kam im Außenbereich und im Gastraum ausschließlich § 6b BDSG in Betracht, da es sich bei dem äußeren Sitzbereich und dem Gastraum eines Restaurants um öffentlich zugängliche Räumlichkeiten handelt. Unter einem öffentlich zugänglichen Bereich versteht man jeden Raum, der einem unbestimmten Personenkreis zugänglich ist. Die Überwachung solcher Bereiche ist nur im Rahmen einer Erforderlichkeit des abschließenden Zweckkatalogs des § 6b Abs. 1 Nr. 1 bis 3 BDSG zulässig. Vorliegend verblieb nur nach Nummer 2 eine Videoüberwachung für die Zwecke des Hausrechts. Allerdings mangelte es diesem Zweck bereits an der notwendigen Erforderlichkeit. Diese ist nur dann gegeben, wenn die Kameraüberwachung zur Erreichung dieses Zwecks geeignet ist und kein milderes Mittel zur Verfügung steht, um den angestrebten Zweck bei gleicher Effektivität zu erreichen. Die hier durchgeführte Videoüberwachung war jedoch bereits nicht zur Wahrnehmung des Hausrechts geeignet. Die Ausübung des Hausrechts richtet sich immer gegen einen unmittelbar bevorstehenden oder gegenwärtigen Angriff auf Rechtspositionen des Hausrechtsinhabers. Die Videoüberwachung, wie sie hier betrieben wurde, war aber nicht so ausgestaltet, dass durch die Überwachung aufgezeichnete Vorgänge unmittelbar wahrgenommen werden konnten bzw. auf diese reagiert werden konnte. Zugriffe auf die in der Anlage gespeicherten Videos sollten vielmehr mit mobilen Endgeräten und in der Regel zu einem späteren Zeitpunkt erfolgen. Dann ist aber eine Durchsetzung des Hausrechts nicht mehr möglich.
Auch aufgrund der Tatsache, dass der Gastraum stets mit mehreren Mitarbeitern besetzt ist, lässt sich so effektiver eine Kontrolle der Gasträume realisieren. Damit fehlte es ebenfalls an der Erforderlichkeit, da auch hier die Kontrolle seitens der Servicemitarbeiter zur Verfolgung des angestrebten Zweckes durchgreifender gewesen wäre, weil ein Mitarbeiter ein von einem Kunden begangenes Fehlverhalten nicht nur besser und zuverlässiger feststellen, sondern auch unmittelbar darauf reagieren könnte.
Allgemein bieten Restaurants und Bars den Gästen einen Raum zur Entspannung und Erholung sowie sonstiger Freizeitgestaltung. Das schutzwürdige Interesse daran, diese Aktivitäten ohne eine andauernde Beobachtung durch Videokameras und den dadurch ausgeübten Überwachungsdruck auszuüben, wird als elementarer Teil des Grundrechts auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 Grundgesetz (GG), Art. 2 Abs. 1 GG. angesehen. Das Interes-

se der Betreiber hingegen an der Durchsetzung ihres Hausrechtes ist Teil der verfassungsrechtlich garantierten Eigentumsfreiheit, Art. 14 Abs. 1 GG, sowie der Berufsfreiheit, Art. 12 Abs. 1 GG. Das schutzwürdige Interesse der Gäste an einer unbeobachteten Freizeitgestaltung überwiegt insoweit das Interesse der Betreiber an einer dauerhaften Beobachtung der Gäste im Barbereich.
Auch die Videoüberwachung in der Küche sowie im Lager der Gaststätte entsprach nicht den Vorgaben des BDSG und war daher nicht zulässig. Bei den Videoaufnahmen der Küche handelte es sich um Räume, die ausschließlich von Mitarbeitern des Restaurants betreten wurden, die sich dort ständig bzw. regelmäßig aufhielten, um ihren arbeitsvertraglichen Pflichten nachzukommen. Auch diese Videokameras haben personenbezogene Daten i. S. d. BDSG erhoben, und auch hier gilt das bereits dargestellte materielle Verbot mit Erlaubnisvorbehalt. Eine Einwilligung der Mitarbeiter lag nicht vor. Da der gesamte hintere Bereich des Restaurants videoüberwacht wurde und von den Mitarbeitern immer zwingend betreten werden musste, handelte es sich im Fall der Videoüberwachung im Lager und in der Küche der Gaststätte um eine Arbeitnehmerüberwachung, die nur unter der Maßgabe des § 32 Abs. 1 Satz 1 BDSG zulässig sein konnte. Die Voraussetzungen der nach § 32 Abs. 1 Satz 1 BDSG zulässigen Arbeitnehmerüberwachung waren jedoch nicht erfüllt. So ist für die Zulässigkeit einer Datenerhebung, -verarbeitung oder -nutzung Voraussetzung, dass diese für Zwecke des Beschäftigungsverhältnisses erfolgt und für dessen Durchführung erforderlich ist. Diese Rechtfertigungsschwelle ist wegen der besonderen Intensität eines durch Videoüberwachung verursachten Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Beschäftigten hoch. Daraus folgt, dass eine präventive Videoüberwachung ohne konkreten Grund den Anforderungen von § 32 Abs. 1 Satz 1 BDSG nicht genügt. Ein konkreter Grund kann zum Beispiel eine derart gefahrengeneigte Tätigkeit in abgelegenen Betriebsbereichen sein, dass eine dauerhafte Beobachtung der Arbeitnehmer zum Zwecke der Arbeitssicherheit erforderlich ist. Von einer solchen Erforderlichkeit ist bei einem Restaurantbetrieb jedoch nicht auszugehen. Weder sind die Arbeiten derart gefahrengeneigt, noch ist das Arbeitsumfeld abgelegen.
Daraufhin meldete sich der Rechtsanwalt des Gaststättenbetriebes und erhob Klage gegen den Anordnungsbescheid des TLfDI. Beim TLfDI kann der Adressat des Verwaltungsaktes nicht, wie norma-

lerweise in einem Verwaltungsverfahren üblich, zunächst Widerspruch gegen den Verwaltungsakt einlegen, sondern muss innerhalb eines Monats nach Zustellung des Bescheids schriftlich oder zur Niederschrift des Urkundsbeamten der Geschäftsstelle Klage beim zuständigen Verwaltungsgericht erheben.
Die Klage begründete der Rechtsanwalt damit, dass die vom TLfDI gerügte Videoüberwachung mittels der Kameras rechtmäßig sei. Die Kameras seien deswegen zulässig, weil seitens des Restaurantbetreibers ein berechtigtes Überwachungsinteresse wegen der Verhinderung bzw. Aufklärung von Straftaten vorliege.
Die Rechtsauffassung des TLfDI wurde mit Urteil des Verwaltungsgerichts Weimar vom 4. November 2015 bestätigt. Das Urteil ist aber noch nicht rechtskräftig.

Die Videoüberwachung muss für den von ihr verfolgten Zweck geeignet und erforderlich sein. Videokameras in Gaststätten, die im Gastraum installiert sind und auch den öffentlich zugänglichen Außenbereich aufzeichnen, sind in der Regel datenschutzrechtlich unzulässig. § 32 Bundesdatenschutzgesetz (BDSG) regelt, dass das Erheben und Verarbeiten von Arbeitnehmerdaten nur dann zulässig ist, wenn dies für die Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Bei einer Videoüberwachung ist dies in der Regel nicht der Fall. Daher gilt: Jede Videokamera, die auf Arbeitsplätze oder sonstige Orte gerichtet ist, an denen sich Arbeitnehmer regelmäßig aufhalten, ist unzulässig.

4.81 Drohende Drohnen – Videogaga 78

Der Thüringer Landesbeauftragte für den Datenschutz (TLfDI) beobachtet die Entwicklung an der Drohnenfront mit Sorge. Die kleinen wendigen Fluggeräte mit Kameraausstattung sind inzwischen zu immer niedrigeren Preisen käuflich zu erwerben. Die teureren Geräte besitzen dabei Videokameras, die Aufnahmen in hoher Auflösung erstellen können. Da der Luftraum im Regelfall keine physischen Grenzen hat, können die Drohnen auf einfache Weise in Örtlichkeiten vordringen, die eigentlich höchstprivat bleiben sollen. Dies kann ebenso die Beobachtung von fremden Grundstücken wie auch von FKK-Bereichen am See oder sonstiger nicht einfach zugänglicher Bereiche sein. Auch die Bewohner von Hochhäusern können sich nicht mehr sicher sein, ob eine geschlossene Gardine notwendig ist,

weil ja eigentlich niemand Einsicht nehmen kann. Einerseits ist aus datenschutzrechtlicher Sicht klar, dass solche Beobachtungen durch private Drohnen ohne Einwilligung der hiervon Betroffenen unzulässig sind. Andererseits handelt es sich um ein relativ neues Phänomen, auf das der Gesetzgeber noch nicht mit verbindlichen eindeutigen Regelungen speziell für Drohnen im zivilen Bereich reagiert hat. Die herkömmlichen Vorschriften, die für die Beurteilung der Zulässigkeit herangezogen werden können, sind das Recht am eigenen Bild gemäß § 22 des Kunsturhebergesetzes sowie das Grundrecht auf informationelle Selbstbestimmung. Selbst wenn alle hier denkbaren datenschutzrechtlichen Erlaubnisnormen, etwa § 6b, § 28 sowie § 32 Bundesdatenschutzgesetz, einschlägig wären, ist der TLfDI der Auffassung, dass im Regelfall die schutzwürdigen Interessen des Betroffenen überwiegen. Folglich darf mit der Kameradrohne grundsätzlich niemand gegen seinen Willen gefilmt werden. Der TLfDI hat einen Beschlussentwurf zur Nutzung von Kameradrohnen durch Private in den Kreis der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) eingebracht. Dieser Beschluss ist inzwischen veröffentlicht worden und z. B. unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2015/Nutzung_von_Kameradrohnen_durch_Private1/Beschluss_Drohnennutzung_durch_Private.pdf abrufbar. (siehe auch unter Anlage 8).

Hierin wird unter anderem darauf hingewiesen, welche Möglichkeiten bestehen, um einem unzulässigen Einsatz von Drohnen im privaten Bereich zu begegnen. Dies ist etwa das Tätigwerden der zuständigen Aufsichts- und Bußgeldbehörden, die Anordnungen treffen und Bußgeldbescheide gegenüber den „Drohnenführern“ erlassen können. Darüber hinaus können Betroffene dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht auch zivilrechtlich begegnen. Hier kann den Betroffenen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Droht sogar mit dem Drohneneinsatz die Verwirklichung von Straftatbeständen, etwa die Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche nach § 201a Strafgesetzbuch (StGB) oder des nicht-

öffentlich gesprochenen Wortes nach § 201 StGB, so können ebenfalls die Strafverfolgungsbehörden eingeschaltet werden. Es sind daher alle Drohnenbetreiber aufgefordert, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Auch auf europäischer Ebene ist die bestehende Problematik erkannt und aufgegriffen worden. So hat die Europäische Kommission einen neuen Rechtsrahmen für den Betrieb ziviler Drohnen vorgeschlagen, um die uneingeschränkte Anwendung der Datenschutzbestimmungen auf pilotenferngesteuerte Luftfahrzeuge zu gewährleisten. Auch der Europäische Datenschutzbeauftragte hat in einer Stellungnahme zur Absichtserklärung der Europäischen Kommission darauf hingewiesen, dass Drohnen die Verarbeitung von mehr personenbezogenen Daten als Flugzeuge und Videoüberwachungsanlagen ermöglichen und die Nutzung von Drohnen zu zivilen Zwecken die Grundrechte auf Privatsphäre und Datenschutz respektieren muss. Der TLfDI wird sich für die Schaffung einer speziellen datenschutzrechtlichen Regelung für den privaten Drohneneinsatz einsetzen und im Übrigen als für den Datenschutz zuständige Aufsichtsbehörde bei einer unzulässigen Erhebung oder Verarbeitung von Daten unter Verwendung von Drohnen auch Bußgelder verhängen.

Der Einsatz von Drohnen hat in vielen Bereichen seine Berechtigung und kann von großem Nutzen sein, etwa bei Katastropheneinsätzen, im Straßen- und Eisenbahnbrückenbau oder für die Forst- und Landwirtschaft. Die Erhebung und Verarbeitung personenbezogener Daten bei der privaten Verwendung von Drohnen ist aber kritisch zu sehen. Grundsätzlich darf niemand Personen und deren höchstpersönlichen Lebensbereich ohne deren Wissen oder gegen ihren Willen fotografieren oder filmen.

4.82 Lebensmittel vor der Kamera – oder doch nur Mitarbeiterüberwachung? – Videogaga 79

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) meldete sich ein Arbeitnehmer und zeigte an, dass bei seinem Arbeitgeber – einer Nahrungsmittel-GmbH – in der Produktionshalle eine Domekamera mit 360 Grad Blickrichtung installiert sei, mittels derer eine Überwachung der dort tätigen Mitarbeiter erfolgte. Zeitgleich bat der Arbeitnehmer um eine anonyme Bearbeitung seiner Beschwerde. Noch bevor der TLfDI

den Arbeitgeber mit einem umfassenden Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) zur streitgegenständlichen Domekamera in der Produktionshalle anschreiben konnte, meldete sich der Arbeitnehmer erneut beim TLfDI. Er führte aus, dass sein Arbeitgeber nun neben der Domekamera auch Wildkameras in den Produktionshallen aufgebaut habe.
Daher führte der TLfDI eine Kontrolle bei der Nahrungsmittel-GmbH durch. Bei der Inaugenscheinnahme vor Ort machte der TLfDI folgende Feststellungen:
Nach einem Brand in der Vergangenheit, bei dem 90 % der Gebäude zerstört worden waren, wurde der Betrieb von der Nahrungsmittel-GmbH neu aufgebaut. Daraufhin erhielt der Betrieb die International Featured Standards (IFS)-Zertifizierung, die zum Ziel hat, sicherzustellen, dass das Produkt nicht verfälscht oder sabotiert werden kann. Zur Umsetzung der Standardbestimmungen zur IFS-Zertifizierung brachte das Unternehmen zwei Domekameras an, die auch die an den Standorten beschäftigten Mitarbeiter erfassten. Die Domekamera in der Halle, in der die abgepackten Paletten zur Abholung bereitgestellt werden, dient nach Angaben der Nahrungsmittel-GmbH dem Schutz vor unbefugtem Eindringen und zur Kontrolle der Zugänge, um den Erfordernissen der IFS-Standards (hier Zutrittskontrolle und Identifizierbarkeit von Besuchern und Externen) nachzukommen. Vor allem habe es nach Angabe des Unternehmens in der Halle in der Vergangenheit mehrfach Beschwerden von Bestellern gegeben, dass ganze Paletten oder nur Teile der Produkte beschädigt waren. Auch seien ca. 100 Kartons der abgepackten Produkte abhandengekommen.
Die installierte Domekamera in der anderen Halle war aus Sicht des Unternehmens ein geeignetes Verfahren, um im Sinne der IFS-Standards zur Qualitätssicherung eine Fälschung/Sabotage der Produkte zu verhindern und die Identifizierung von Anzeichen für Sabotage zu ermöglichen. In der Vergangenheit habe man einmal rote Kügelchen im Endprodukt gefunden, die nicht deklariert waren. Um Derartiges zu vermeiden oder zumindest nachzuvollziehen, sei die Kameraüberwachung erforderlich.
Auf die Videoüberwachung werde an den Eingängen zu den jeweiligen Betriebsbereichen durch Beschilderung hingewiesen. Die Mitarbeiter werden in allgemeiner Form über die Sicherheitsaspekte in der Firma belehrt, eine konkrete Dokumentation zur Videoinstallation ist jedoch nicht vorhanden.

Der TLfDI erläuterte die Rechtslage wie folgt: Eine Videokamera, so auch eine Domekamera, ist eine Überwachungsanlage. Ihr bleibt nichts verborgen. Gerade am Arbeitsplatz stoßen zudem die Interessen von Arbeitnehmer und Arbeitgeber aufeinander. Die Aufzeichnung von Bildern stellt eine Datenerhebung von personenbezogenen Daten dar, die nach § 4 Abs. 1 BDSG nur zulässig ist, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt.
Die Videoüberwachung in beiden Hallen erfasst auch Mitarbeiter, sodass eine Datenerfassung nach § 32 BDSG vorliegt. Eine offene Videoüberwachung auf dieser Rechtsgrundlage ist aber nur dann zulässig, wenn die Mitarbeiter nicht im Fokus der Überwachung stehen und mit ihr besondere Schutzpflichten des Arbeitgebers gegenüber dem Betroffenen erfüllt werden müssten, insbesondere in besonders gefahrträchtigen Arbeitsbereichen. Dies lag nach Ansicht des TLfDI augenscheinlich hier nicht vor und wurde auch nicht von der Nahrungsmittel-GmbH so vorgetragen. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nach § 32 Absatz 1 Satz 2 BDSG nur dann erhoben, verarbeitet und genutzt werden, wenn vorab dokumentierte tatsächliche Anhaltspunkte den Verdacht begründen, dass ein bestimmter Betroffener im Beschäftigungsverhältnis eine Straftat begangen hat. Wesentlich ist, dass sich ein bestimmter Verdacht gegen einen bestimmten Beschäftigten richten muss. Auch dies war vorliegend nicht gegeben.
Soweit eine Videoüberwachung in nicht-öffentlichen Räumen nicht im Zusammenhang mit dem Beschäftigungsverhältnis steht, kann sie nach § 28 Absatz 1 Satz 1 Nr. 1 BDSG zulässig sein. Der Einsatz der Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und die schutzwürdigen Belange des Beschäftigten dürfen nicht überwiegen. Daher können auch Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Vordergrund der Überwachung steht und nicht permanent erfasst wird. Jedoch ist zu überprüfen, ob weniger einschneidende Mittel zur Verfügung stehen. Nach der Rechtsprechung kann die Überwachung von Beschäftigten zulässig sein, wenn sie offen erfolgt, der Arbeitgeber ein berechtigtes Interesse an den Kameraaufnahmen hat, beispielsweise, um Diebstählen oder Vandalismus, aber auch Sabotageakten durch sein Personal vorzubeugen. Erforderlich ist in einem solchen Fall die Abwägung der Interessen des Arbeitgebers mit den schutzwürdigen Belangen der betroffenen Mitarbeiter. Das Persönlichkeitsrecht schützt den Be-

schäftigten vor einer lückenlosen Überwachung und damit vor einem permanenten Überwachungsdruck durch Videoüberwachung, dem er sich nicht entziehen kann. Verbleibt dem Beschäftigten ein unbeobachteter Arbeitsbereich und sind sensible Bereiche wie Sanitär- und Pausenräume etc. von der Überwachung ausgenommen, kann die Abwägung zugunsten des Arbeitgebers ausfallen.
Obwohl es sich bei den installierten Kameras nach dem äußeren Eindruck um Domekameras handelte, die grundsätzlich eine große Rundum-Erfassung ermöglichen können, wurde tatsächlich jeweils nur ein kleiner Ausschnitt der Produktionshalle und des Lagerausgangs erfasst. Die Videoüberwachung diente nicht in erster Linie der Überwachung der dort tätigen Mitarbeiter, sondern der Qualitätssicherung in der Produktion und der Dokumentation des unversehrten Verlassens der Produkte aus der Lagerhalle. In die notwendige Abwägung des Interesses des Unternehmens mit dem schutzwürdigen Interesse der Betroffenen war zugunsten der Nahrungsmittel-GmbH zu berücksichtigen, dass keine permanente Überwachung des gesamten Arbeitsbereiches stattfand. Die Videoüberwachung wurde nur in den eingegrenzten Bereichen durchgeführt. Durch die Einstellung der Kameras erfolgte eine Erfassung der Mitarbeiter nur, soweit dies aufgrund der Bedienung der Maschinen nicht vermeidbar ist. In Anbetracht der beschränkten Erfassungsbereiche kann die Videoüberwachung daher zum Schutz vor Sabotage im berechtigten Interesse des Unternehmers als grundsätzlich geeignet angesehen werden. Die erforderlichen formalen Zulässigkeitsvoraussetzungen (Verzeichnis der Kameras mit der Angabe des jeweiligen konkreten Zwecks und des Erfassungsbereichs) werden derzeit von dem Unternehmen abgearbeitet.

Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten der Beschäftigten durch eine Videoanlage kann in der Regel nicht auf § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) gestützt werden. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art

und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

4.83 Essen in der Werkhalle verboten – Videogaga 80

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine anonyme Beschwerde über ein mittelständiges produzierendes Unternehmen. Das Unternehmen überwache seine Mitarbeiter mit Videotechnik. Zunächst hätte es nur einige Kameras gegeben. Vor kurzem sei die Zahl der Kameras aber erhöht worden. Der Arbeitgeber benutze Videoüberwachung offenbar zur Mitarbeiterüberwachung. So sei beispielsweise der Werkleiter aufgefordert worden einzuschreiten, weil ein Mitarbeiter in der Produktionshalle esse.
Der TLfDI führte in dem Unternehmen eine Vorortkontrolle durch. Es wurden umfangreiche datenschutzrechtliche Mängel festgestellt.
Im Unternehmen waren ca. 10 bis 15 Personen mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigt. Nach § 4f Abs. 1 Bundesdatenschutzgesetz (BDSG) haben nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich zu bestellen. Da in dem Unternehmen mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt waren, bestand die Pflicht zur Bestellung eines Datenschutzbeauftragten, den es in dem Unternehmen aber nicht gab. Es bestand ein Vertrag mit einem externen Lohnbüro, das sowohl die Lohn- und Gehaltsabrechnung vornahm als auch die Personalaktenführung. Die Verarbeitung von Personaldaten durch ein externes Lohnbüro stellt eine Auftragsdatenverarbeitung dar, bei der der Auftraggeber für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich bleibt, § 11 Abs. 1 Satz 1 BDSG. Nach § 11 Abs. 2 BDSG ist der Auftrag schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Vertrag zur Auftragsdatenverarbeitung mit dem externen Lohnbüro konnte bei der Kontrolle nicht vorgelegt werden. Ein IT-Sicherheitskonzept existierte im Unternehmen nicht. Ein Konzept zur Löschung und Sperrung von Daten gab es in schriftlicher Form nicht. Ein Notfallplan zu § 42a BDSG existierte nicht. Eine schriftliche Festlegung zu den Zugriffsrechten zu den automatisiert verarbeiteten Daten gab es ebenfalls nicht. Nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten, § 9 BDSG. In den technisch-organisatorischen Maßnahmen müssen Festlegungen zur Absicherung des internen lokalen Netzes (z. B. Firewall, Schutzsoftware vor Schaden stiftenden Programmen, sicherheitstechnische Einstellungen der Software etc.) getroffen werden. Des Weiteren sind Aussagen zu eventuellen Protokollierungen, zu Datensicherung oder -analysen und gegebenenfalls Festlegungen zur Wartung und Fernwartung seitens Fremdfirmen erforderlich. Dabei müssen die Verfahren jederzeit, insbesondere bei Änderungen und Weiterentwicklungen der IT-Infrastruktur, dem Stand der Technik und den aktuellen Gegebenheiten angepasst werden können. Es ist sicherzustellen, dass die technisch-organisatorischen Maßnahmen der aktuellen Organisationsstruktur des Unternehmens und dem jeweiligen Stand der Technik entsprechen. Zu diesem Zweck sind die Maßnah-

men und Festlegungen zum Datenschutz und der Datensicherheit in regelmäßigen Abständen auf ihre Aktualität und Wirksamkeit zu überprüfen und ggf. zu überarbeiten und zu ergänzen. Regelungen sind auch zur Versendung von E-Mails mit personenbezogenen Daten zu treffen. Auch die bestehenden unterschiedlichen Zugriffsrechte der Mitarbeiter sind schriftlich zu fixieren.
Innerhalb des Unternehmens fand außerdem eine Videoüberwachung statt. Die Videotechnik wurde von einer Sicherheitsfirma installiert und die Anlage von dieser Firma gewartet. Die Bilder wurden im Unternehmen erhoben. Die Videoüberwachung erfolgte nach Angaben des Unternehmens „aus Sicherheitsgründen“. Genauere schriftliche Angaben zum konkreten Zweck der Videoüberwachung wurden nicht gemacht. Schriftliche Festlegungen gab es zur Videoüberwachung überhaupt nicht. Die Bilder waren nicht live zu beobachten, sondern liefen auf einem Server auf. Die Speicherdauer war dem Unternehmen bei der Kontrolle nicht bekannt.
Das Unternehmen wurde aufgefordert, einen betrieblichen Datenschutzbeauftragten (bDSB)zu bestellen, ein IT-Sicherheitskonzept zu erstellen, Verträge zur Auftragsdatenverarbeitung mit dem externen Lohnbüro sowie mit der Sicherheitsfirma vorzulegen sowie genaue Angaben zu den eingesetzten Kameras zu machen. Dabei sind die Kameras einzeln aufzuführen, für jede Kamera ist gesondert der Zweck der Videoüberwachung anzugeben und es ist zu jeder Kamera ein Screenshot des Aufnahmebereichs einzureichen. Die pauschale Angabe der „Sicherheitsgründe“ ist jedenfalls völlig unzureichend.
Nach Übermittlung der geforderten Unterlagen wird der TLfDI die Rechtmäßigkeit der eingesetzten Videoüberwachung prüfen. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten mittels Videoüberwachung ist nur zulässig, soweit ein Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Eine Einwilligung kommt bei der Videoüberwachung in aller Regel nicht in Betracht. Im Hinblick auf die Beschäftigten scheitert eine wirksame Einwilligung wegen des abhängigen Beschäftigungsverhältnisses bereits an der erforderlichen Freiwilligkeit, § 4a Abs. 1 Satz 1 BDSG. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG für die Videoüberwachung von öffentlich zugänglichen Räumen. In sonstigen Bereichen kann eine Videoüberwachung nach den Regelungen der §§ 28 und 32 BDSG zulässig sein. Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten der Beschäftigten durch eine Video-

anlage kann in der Regel nicht auf § 32 Absatz 1 Satz 1 BDSG gestützt werden. Nach dieser Regelung muss die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich sein. Denkbar sind allenfalls offene Überwachungsmaßnahmen insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Ob diese Voraussetzungen vorliegen, wird zu prüfen sein. Der TLfDI wird ebenfalls die Einleitung eines Ordnungswidrigkeitenverfahrens wegen der festgestellten Verstöße prüfen.

Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der datenschutzrechtlichen Vorschriften zu gewährleisten, § 9 BDSG. In den technisch-organisatorischen Maßnahmen müssen Festlegungen zu allen mit personenbezogenen Daten verbundenen technischen Abläufen im Unternehmen getroffen werden. Im Fall einer Videoüberwachung ist für jede Kamera gesondert der mit ihr verfolgte Zweck festzulegen.

4.84 Attrappe im Hausflur – Videogaga 81

Immer häufiger passiert es, dass Hausverwaltungen in Mehrfamilienhäusern zur Verhinderung von Sachschäden auf den Einsatz von Videokameras zurückgreifen. Mieter fühlen sich bisweilen von der mitunter in sehr drohendem Tonfall angekündigten Maßnahme in die Ecke gedrängt. So auch ein Mieter, der sich hilfesuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte. Nach seinem Vortrag hatte die Hausverwaltung zunächst die Videoüberwachung des Hauses, in dem er wohnte, angekündigt und dann eine Kamera im Hausflur angebracht. Auf seine Bitte um Auskunft zur Videoüberwachung reagierte die Hausverwaltung nicht. Der TLfDI wandte sich mit einem Auskunftsersuchen an die Hausverwaltung, die dieses zunächst für einen Faschingsscherz hielt, da das Schreiben auf den 11. November des Jahres datiert war. Nachdem ein neuerliches Schreiben mit Postzustellungsurkunde an die Geschäftsleitung gerichtet wurde, reagierte

das Unternehmen. Es teilte mit, dass nicht die Hausverwaltung, sondern die Eigentümergemeinschaft des Hauses eine Videoüberwachung durchführen wolle. Im Objekt habe es mehrere Straftaten gegeben. Die Fragen des TLfDI zur Videoüberwachung könnten nicht beantwortet werden, weil keine aktive Kamera betrieben werde. Es sei aber die Anschaffung und der Betrieb einer aktiven Kamera geplant, insofern wurde um Beratung ersucht, welche Vorgaben zu beachten wären.

Diese Äußerung konnte dahingehend verstanden werden, dass eine Kameraattrappe aufgehängt worden war. Der TLfDI wies darauf hin, dass das einschlägige Bundesdatenschutzgesetz (BDSG) den Zweck hat, das Grundrecht auf informationelle Selbstbestimmung zu gewährleisten. Dieses vom Bundesverfassungsgericht in seiner Entscheidung zur Volkszählung vom 15. Dezember 1983 weiterentwickelte Grundrecht auf informationelle Selbstbestimmung beinhaltet auch einen Schutz gegen Kameraattrappen. Dies begründet sich in dem von solchen Einrichtungen ausgehenden Überwachungsdruck. Nach Auffassung des TLfDI beurteilen sich Attrappen daher grundsätzlich nach den gleichen Maßstäben wie tatsächlich funktionsfähige Kameras, da von ihnen bereits ein Überwachungsdruck ausgeht. Das Unternehmen sollte daher darlegen, ob eine Kameraattrappe in dem Gebäude installiert wurde, welchen Zweck und welchen vermeintlichen Aufnahmebereich sie hat.

Zur Frage der Verantwortlichkeit für die Videoüberwachung gilt Folgendes:

Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Sofern die Eigentümergemeinschaft die Hausverwaltung mit dem Betrieb einer Videoüberwachungsanlage beauftragt hat, muss ein Vertrag nach § 11 BDSG zur Datenverarbeitung im Auftrag vorliegen und dem TLfDI vorgelegt werden.

Zur Zulässigkeit der Videoüberwachung verwies der TLfDI auf die Orientierungshilfe „Videoüberwachung bei nicht-öffentlichen Stellen“, die vom so genannten Düsseldorfer Kreis erarbeitet worden ist. Der Düsseldorfer Kreis ist ein Zusammenschluss aller Aufsichtsbehörden für den Datenschutz in Deutschland. Die dort niedergelegten Grundsätze legen einheitliche Anforderungen an die Videoüberwachung durch nicht-öffentliche Stellen dar, die auch in Thüringen gelten. Aus der Orientierungshilfe ergibt sich, dass ein berechtigtes

Interesse für den Betrieb einer Videoüberwachungsanlage im Sinne von § 6b Abs. 1 Nr. 3 BDSG ideeller, wirtschaftlicher oder rechtlicher Natur sein kann. Soll die Videoüberwachung wie im vorliegenden Fall dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit. Derartige Nachweise wurden vom Unternehmen angefordert. Erst wenn alle Informationen vorliegen, kann das Verfahren abgeschlossen werden.

Das Grundrecht auf informationelle Selbstbestimmung beinhaltet auch einen Schutz gegen Kameraattrappen. Dies begründet sich in dem von solchen Einrichtungen ausgehenden Überwachungsdruck. Wird ein Unternehmen mit der Durchführung der Videoüberwachung beauftragt, muss der entsprechende Vertrag den Anforderungen des § 11 BDSG genügen.

4.85 1, 2, 3: Das Filmen ist noch nicht vorbei! – Videogaga 82 falsche Auskünfte gegenüber TLfDI

Die meisten Menschen sehen die Beobachtung durch eine Videokamera als die unangenehmste Art der Überwachung an, weil sie so umfassend ist. Es wird dabei schließlich nicht nur ein einfaches Protokoll mit wenigen technischen Informationen erstellt, sondern jede Bewegung und jeder Gesichtsausdruck aufgezeichnet. Da dies einen schwerwiegenden Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt, ist eine Videoüberwachung nur dann zulässig, wenn für den konkreten Fall eine entsprechend Rechtsgrundlage oder Einwilligung der betroffenen Personen, was fallbezogen bei der Videoüberwachung wirklichkeitsfremd wäre, vorliegt.
Erneut beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einer Beschwerde über die Videoüberwachung eines Grundstücks. Am Haus hatte der Eigentümer insgesamt vier Kameras installiert. Direkt gegenüber vom Grundstück befand sich ein 24-Stunden-Getränkeladen. Nach Aussage des Eigentümers versorgten sich die Jugendlichen dort regelmäßig mit alkoholischen Getränken und würden sich an-

schließend auf der Treppe seines Hauses niederlassen, um die Getränke dort zu konsumieren.
Daraufhin forderte der TLfDI den Grundstückseigentümer auf, einen Fragenkatalog unter anderem zum Zwecke der Videoüberwachung zu beantworten sowie die angeforderten Nachweise, wie z. B. ein von der Kamera aufgenommenes Bild und ein Foto des Hinweisschildes beim TLfDI einzureichen. Der Grundstückseigentümer teilte dem TLfDI mit, dass er das ebenfalls auf seinem Grundstück betriebene Büro geschlossen habe. Daher unterhalte er keine Kameras mehr. Trotzdem benannte der Eigentümer als Zweck der Videoüberwachung den Schutz vor Vandalismus und ähnlichen Vorkommnissen zu seinen Lasten.
Bei der Videobeobachtung werden personenbezogene oder -beziehbare Daten gespeichert. Personenbezogene oder -beziehbare Daten sind im Sinne des Bundesdatenschutzgesetzes (BDSG) dabei alle Informationen, die eine Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person enthalten, § 3 Abs. 1 BDSG. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm inner- oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Da eine Einwilligung bei Videoüberwachungsanlagen naturgemäß ausscheidet, bleibt es bei der Notwendigkeit einer Rechtsvorschrift. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist daher § 6b BDSG, welcher die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen abschließend regelt. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen.
Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Vandalismus zu schützen, ist

darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.
Solche konkreten Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder Vorkommnisse in der Vergangenheit, konnte der Grundstückseigentümer dem TLfDI bisher nicht nachweisen.
Aufgrund der Angabe des Betreibers der Kameras, dass er die Videoüberwachungsanlagen zwischenzeitlich demontiert habe, wandte sich der TLfDI im Rahmen der Amtshilfe mit der Bitte, zu ermitteln, ob die Kameras zwischenzeitlich entfernt worden sind, an die Stadtverwaltung Erfurt.
Infolgedessen stellte die Stadtverwaltung Erfurt bei der durchgeführten Vorortkontrolle fest, dass am Gebäude insgesamt noch vier Videokameras angebracht waren, ausgerichtet in verschiedene Richtungen.
Der TLfDI beabsichtigt daher, den Betreiber aufzufordern, die Videokameras sofort zu entfernen. Wegen der darüber hinaus möglicherweise vorliegenden Falschauskunft des Betreibers der Kameras sowie möglicher weiterer Verstöße gegen das Datenschutzrecht wird die Einleitung eines Ordnungswidrigkeitenverfahrens geprüft.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. In der Regel verstößt das Ausrichten einer Videokamera auf eine öffentliche Straße oder einen öffentlichen Fußweg gegen das Datenschutzrecht.

4.86 Bitte lächeln: Kameras im Kino – Videogaga 83

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil in einem Kino nicht nur Filmvorführungen gemacht würden, sondern auch Videoaufzeichnungen. Das Kino sei mit vier Kameras ausgestattet, eine Kamera gäbe es am Seiteneingang und drei Kameras im Foyer des Hauses. Diese Angaben bestätigten sich bei einer Vorortkontrolle des TLfDI. Im Kino wurden vier Kameras betrieben. Eine Kamera

befand sich im Eingangsbereich, sie war vom Eingang her auf die Theke gerichtet, an der die Besucher Getränke und Knabbereien sowie auch Eintrittskarten kaufen konnten. Sie nahm in erster Linie das Geschehen vor der Theke auf. Im Aufnahmebereich waren außerdem die Beschäftigten hinter der Theke teilweise zu erkennen Eine weitere Kamera war so montiert, dass sie den Thekenbereich von hinten aufnahm. Die Beschäftigten waren bei ihrer Tätigkeit hinter der Theke permanent der Überwachung ausgesetzt, ohne eine Ausweichmöglichkeit zu haben. Weniger als die Hälfte des Bildausschnittes richtete sich auf den Bereich für das Publikum. Außerdem wurde ein Teil des Bereichs mit aufgenommen, in dem sich Sitzgelegenheiten für die Gäste des Kinos befanden. Die dritte Kamera war von hinten direkt in den Bereich gerichtet, in dem Kunden Karten kauften. Dabei nahmen über zwei Drittel des Bildes den Bereich ein, in dem sich die Beschäftigten aufhielten, lediglich ein Drittel den Bereich mit Publikumsverkehr. Die letzte Kamera befand sich im Hausflur des Hauses, in dem das Kino betrieben wird. Sie ist auf die Eingangstür und die Briefkästen gerichtet. Die Kameraanlage wurde durch eine externe Firma installiert. Diese Firma wartete und betreute die Anlage auch. Der Vertrag mit dieser Firma konnte bei der Kontrolle nicht vorgelegt werden. Die Ansichten der Videoaufzeichnungen konnten über einen Laptop vor Ort angesehen werden. Über die verschiedenen Bedienungsfunktionen des Programms konnten bei der Kontrolle keine Angaben gemacht werden, es wurde auf die externe Dienstleistungsfirma verwiesen.

Als Grund für das Anbringen der drei Kameras im Foyer des Kinos wurde angeben, dass ein Beschäftigter des Kinos während seiner Arbeitszeit einem tätlichen Angriff ausgesetzt gewesen war. Einen Einbruch habe es im Kino bislang nicht gegeben. Die drei Kameras im Kino selbst sollten insbesondere auch dazu dienen, mögliche Täter eines Einbruchs bei ihrer Flucht aufzeichnen zu können. Außerdem sollte einem möglichen Diebstahl vorgebeugt werden, der insbesondere dann stattfinden könnte, wenn sich nur noch der letzte Mitarbeiter und die Saalreinigungskraft im Gebäude befänden. Die Kamera im Hausflur sei angebracht worden, weil es Probleme mit einem Mieter des Hauses gegeben hätte. Andere Mieter hätten sich darüber beschwert, dass dieser Mieter randaliert habe. Dieser Mieter sei aber mittlerweile ausgezogen. Schriftliche Festlegungen im Hinblick auf die Videoüberwachung existierten nicht.

Nach der Kontrolle forderte der TLfDI den Betreiber des Kinos auf, den mit der externen Firma geschlossenen Vertrag vorzulegen. Der Betreiber wurde dabei auf die Möglichkeit hingewiesen, alle Passagen zu schwärzen, die für die datenschutzrechtliche Beurteilung nicht erforderlich sind (beispielsweise zu zahlende Honorare). Außerdem wurde der Betreiber aufgefordert, nähere Nachweise zu dem tätlichen Angriff auf den Beschäftigten zu erbringen, beispielsweise das polizeiliche Aktenzeichen. Der Betreiber des Kinos teilte neben dem polizeilichen Aktenzeichen mit, dass es mit der externen Firma keinen Vertrag gäbe. Sollte ein Zugriff auf das aufgezeichnete Material notwendig werden, würde der Geschäftsführer der Firma kontaktiert. Dessen Mitarbeiter sichteten dann das Videomaterial.
Der TLfDI recherchierte dann zunächst bei der Polizei und Staatsanwaltschaft zu den Hintergründen des Angriffs auf den Beschäftigten des Kinos. Nach dem von der Staatsanwaltschaft ermittelten und auch dem rechtskräftigen Urteil gegen den Täter zugrunde gelegten Sachverhalt hatte der Angriff Gründe, die im persönlichen Umfeld des Beschäftigten lagen und nicht mit der Tatsache zusammenhingen, dass der Beschäftigte in einem Kino arbeitet und dort ein größeres Risiko von Angriffen besteht. Bei seiner rechtlichen Bewertung kam der TLfDI zu dem Schluss, dass die Videoüberwachung nicht zulässig ist.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Einwilligung kommt nicht in Betracht. Sie ist nach § 4a Abs. 1 BDSG nur wirksam, wenn sie auf einer freien Entscheidung des Betroffenen beruht und er vorab auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen wurde. Die Einwilligung bedarf üblicherweise der Schriftform. Eine etwaige arbeitgeberseitig eingeholte Einwilligung der Beschäftigten ist irrelevant, da es im Beschäftigungsverhältnis an der Freiwilligkeitsvoraussetzung des § 4a Abs. 1 Satz 1 BDSG mangelt. Auch wird im Vorfeld nicht eine Einwilligung aller potentiell von der Videoüberwachung Betroffenen eingeholt. Daher bedarf es zur Rechtmäßigkeit der Durchführung der Videoüberwachung einer gesetzlichen Grundlage. Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welcher die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Diese

Vorschrift gilt für alle Kameras, die Bereiche überwachen, die Kunden oder im Hausflur auch Mietern und deren Besuchern zugänglich sind. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Alle vier in dem Gebäude betriebenen Videokameras zeichnen danach in öffentlich zugänglichen Räumen auf. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Die vom Kinobetreiber angegebenen Gründe rechtfertigen die Videoüberwachung nicht. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Derartige Tatsachen wurden aber nicht vorgebracht. Die Gründe für den Angriff auf den Beschäftigten lagen in dessen persönlichem Umfeld. Eine tatsächliche Gefahrenlage war nicht erkennbar. In bestimmten Fällen kann zwar auch eine abstrakte Gefährdungslage ausreichend sein, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die wertvolle Ware verkaufen oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind (z. B. Tankstellen). Eine derartige abstrakte Gefahrenlage besteht aber bei einem Kino nicht. Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden, wie dies hier der Fall ist. In solchen Fällen ist nicht nur die Persönlichkeitssphäre der Kunden betroffen, sondern es kommt auch zu einer Überwachung der dort tätigen Beschäftigten. Zwar kann in solchen Bereichen, in denen die Wahrscheinlichkeit von Straftaten zu einem geschäftstypischen Risiko gehört und die Erfassung der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, in Einzelfällen das berechtigte Interesse des Arbeitgebers, Straftaten

vorzubeugen, überwiegen. So lag der Fall hier aber nicht, da kein geschäftstypisches Risiko nachgewiesen werden konnte. Das Interesse der Beschäftigten, während ihrer Tätigkeit nicht permanent der Videoüberwachung ausgesetzt zu sein, überwog in diesem Fall. Gleiches gilt hinsichtlich des Interesses der Mieter des Hauses und ihrer Besucher im Hinblick auf die im Hausflur angebrachte Kamera. Der TLfDI beabsichtigte, den Betreiber des Kinos zur Deinstallation der Videoüberwachung aufzufordern und hörte ihn nach § 28 Thüringer Verwaltungsverfahrensgesetz an. Die Anhörungsfrist läuft noch. Gleichzeitig prüft der TLfDI die Einleitung eines Ordnungswidrigkeitenverfahrens wegen Verstoßes gegen § 43 Abs. 1 Nr. 2b BDSG. Danach handelt ordnungswidrig, wer entgegen § 11 Abs. 2 Satz 2 BDSG einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt. Die Übermittlung der Aufzeichnungen an eine externe Firma, die auch mit der Auswertung der Daten beauftragt wird, stellt eine Datenverarbeitung im Auftrag dar, die nur mit einem schriftlichen Vertrag, der den Voraussetzungen des § 11 BDSG entspricht, zulässig ist.

Auch in einem Kino darf es Videoaufzeichnungen nur geben, wenn die Voraussetzungen des § 6b BDSG vorliegen. Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden. Werden Videoaufzeichnungen an externe Firmen übermittelt und durch diese ausgewertet, muss ein Vertrag vorliegen, der den Anforderungen des § 11 BDSG entspricht.

4.87 Flower Power – Videogaga 84 – Video im Blumenladen

Bei dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging ein Telefonanruf eines Betroffenen ein. Dieser teilte mit, dass in einem Blumengeschäft drei Videokameras angebracht seien, die sowohl Arbeitsbereiche, Kundenbereiche als auch den Kassenbereich beobachteten. Der TLfDI wandte sich an den Inhaber des Blumengeschäftes mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG). Dieser teilte mit, dass er zwei Blumengeschäfte betreibe und beide Geschäfte videoüberwacht würden. Als Grund für die Videoüberwachung wurde angegeben, dass diese der Sicherheit der Angestellten diene

und auch Diebstähle verhindern sollte. Der eine Laden befände sich in einer Ecke, wo es schon mehrmals zu Einbrüchen gekommen sei. Die Kamera in dem anderen Geschäft diene nur zur Beobachtung der Fläche im Hof, weil diese vom Geschäft aus schlecht einzusehen sei. Im Nachhinein stellte sich heraus, dass an dem einen Standort auch Aufzeichnungen durchgeführt wurden. Leider reichten die vom Inhaber des Blumengeschäfts gemachten Angaben nicht aus, um die Zulässigkeit der Videoüberwachung abschließend beurteilen zu können. Da der Inhaber des Blumengeschäftes auf Schreiben des TLfDI immer nur dann reagierte, wenn ihm diese mit Postzustellungsurkunde zugestellt wurden, und er auch die ihm gestellten Fragen nach § 38 Abs. 3 BDSG nicht oder nur unvollständig beantwortete, leitete der TLfDI schließlich ein Ordnungswidrigkeitenverfahren ein. Nach § 43 Abs. 1 Nr. 10 BDSG handelt ordnungswidrig, wer entgegen § 38 Abs. 3 Satz 1 BDSG eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 50.000 Euro geahndet werden, § 43 Abs. 3 Satz 1 BDSG. Das Ordnungswidrigkeitenverfahren ist noch nicht abgeschlossen.

Auch wenn der Inhaber des Geschäftes ein Bußgeld zahlt, ist er nicht von seiner Auskunftspflicht nach § 38 Abs. 3 BDSG befreit. Er wurde daher vom TLfDI wiederum angeschrieben. Dabei wurden ganz konkrete Fragen gestellt. Insbesondere ist es für den TLfDI wichtig zu wissen, welche Kameras welchen Typs an welchen Standorten installiert sind, ob sie Bilder aufzeichnen und wie lange die Aufzeichnungen gespeichert werden. Auch der Zweck der Videoüberwachung muss für jede Kamera gesondert angegeben werden. Soll eine Videoüberwachung dazu eingesetzt werden, vor Einbrüchen oder Diebstählen zu schützen, ist darin zwar grundsätzlich ein berechtigtes Interesse im Sinne von § 6b BDSG zu sehen. Es müssen jedoch konkrete Tatsachen vorgebracht werden, aus denen sich eine Gefährdung ergibt. Im vorliegenden Fall wurden keine konkreten Nachweise erbracht, dass eine tatsächliche Gefahrenlage bestand.

Nach derzeitigem Kenntnisstand ist daher die dort durchgeführte Videoüberwachung größtenteils unzulässig. Sofern mit dem Inhaber der Blumengeschäfte keine Einigkeit erzielt werden kann, wird der TLfDI die Demontage der Kameras nach § 38 Abs. 5 Satz 1 BDSG in einem Anordnungsbescheid anordnen und die Einleitung eines weiteren Bußgeldverfahrens wegen unbefugter Datenerhebung nach § 43 Abs. 2 Nr. 1 BDSG prüfen.

Die verantwortlichen Stellen sind nach § 38 Abs. 3 Satz 1 BDSG verpflichtet, auf die Fragen des TLfDI fristgerecht und vollständig zu antworten. Sofern sie dieser Verpflichtung nicht nachkommen, kann ein Bußgeld wegen Verstoßes gegen § 43 Abs. 1 Nr. 10 BDSG verhängt werden.

Personal – © Wolfilser / Fotolia.com

5 Beschäftigtendatenschutz

5.1 Mindestlohn versus Datenschutz?

Das Mindestlohngesetz (MiLoG) sieht vor, dass grundsätzlich alle Arbeitnehmer einen bestimmten Mindestlohn für ihre Arbeit erhalten sollen. Nach § 13 MiLoG haften die Handelsunternehmen dafür, dass auch Dienst- und Werkleister, die von ihnen beauftragt werden, ihren beschäftigten Mitarbeitern den Mindestlohn gewähren. Also haftet beispielsweise ein Unternehmen dafür, dass die von ihm beauftragte Spedition ihren Mitarbeitern und ggf. auch dort beschäftigten Leiharbeitern mindestens 8,50 Euro Lohn bezahlt. Mit dieser Regelung wollte der Gesetzgeber die Wirksamkeit des Mindestlohngesetzes stärken.
Das MiLoG enthält jedoch keine Regelung, wie diese Vorgaben überprüft werden können. Einige Firmen wollen daher am liebsten die Lohnzettel der Mitarbeiter der von ihnen beauftragten Unternehmen erhalten. Dies ist datenschutzrechtlich nicht zulässig, da eine Rechtsgrundlage für die Übermittlung von Beschäftigtenlohndaten aus Gehaltsabrechnungen durch den jeweiligen Arbeitgeber an den Auftraggeber fehlt. Auch eine vertragliche Vereinbarung zwischen

Auftraggeber und Arbeitgeber ist kein Ausweg. Es würde dabei eine Regelung getroffen, die zu Lasten von Dritten, nämlich der Beschäftigten, geht.
Eine datenschutzgerechte Möglichkeit besteht darin, anonymisierte Zahlen zu übermitteln. Zulässig ist auch, vom jeweiligen Arbeitgeber eine Verpflichtungserklärung zur Tariftreue und Mindestentlohnung zu verlangen. Da dies jedoch nicht wirksam einen Haftungsausschluss begründen kann, haben die Datenschutzaufsichtsbehörden im Düsseldorfer Kreis (siehe hierzu unter Nummer 17) auf der Sitzung vom 4./5. März 2015 mehrheitlich ein Überprüfungsverfahren empfohlen, das sich wie folgt gestaltet:

1. Übermittlung anonymisierter Daten an Auftraggeber,
2. Festlegung vertraglicher Regelungen zwecks Prüfung, ob Auftragnehmer ihre Verpflichtungen zur Mindestlohngewährung einhalten (z. B. Vereinbarung von Vertragsstrafen),
3. Überprüfung der Mindestlohngewährung durch von Auftragnehmern im Wege der Datenverarbeitung im Auftrag als Vertrauensperson eingeschaltete Wirtschaftsprüfer oder Steuerberater (sog. „Testatlösung“).

Die dritte Stufe sollte aber nach Ansicht des TLfDI erst dann zur Anwendung kommen, wenn sich Zweifel an der Entlohnung ergeben, da mit der Einschaltung der Vertrauenspersonen auch eine Datenübermittlung an Dritte verbunden ist, was einen weiteren schwerwiegenderen Einschnitt in das informationelle Selbstbestimmungsrecht der betroffenen Mitarbeiter darstellen würde.
Über die vom jeweiligen Unternehmen festgelegte Vorgehensweise sollten auch die betroffenen Mitarbeiter rechtzeitig und umfassend informiert werden.

Der Gesetzgeber ist aufgerufen, eine Rechtsgrundlage für die Übermittlung von Beschäftigtendaten zur Überprüfung der Zahlung von Mindestlohn im MiLoG zu schaffen. Bis dahin bietet der Lösungsvorschlag des Düsseldorfer Kreises eine datenschutzgerechte Lösung für den nach dem MiLoG geforderten Nachweis.

5.2 Ausweispflicht gegenüber dem Arbeitgeber?

Immer wieder wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit gefragt, ob denn der Arbeitgeber die Vorlage des Personalausweises verlangen und eine Kopie hier-

von in die Personalakte aufnehmen dürfe. Auch EC-Karten ihrer Beschäftigten möchten die Arbeitgeber in einigen Fällen kopieren.
Nach § 1 Abs. 1 Satz 3 Personalausweisgesetz dürfen vom Personalausweis grundsätzlich keine Kopien gefertigt werden. Eine gesetzliche Ausnahme von diesem Grundsatz für Unternehmen und Arbeitgeber existiert nicht. Bei Zweifeln, ob es sich bei dem (zukünftigen) Arbeitnehmer auch um denjenigen handelt, für den er sich ausgibt, reicht es zur eindeutigen Identifikation völlig aus, in die Identifikationspapiere lediglich Einsicht zu nehmen, ohne eine Kopie anzufertigen. Im Übrigen würden durch die Ablichtungen der auf einem Personalausweis enthaltenen personenbezogenen Einzelheiten mehr Angaben gespeichert, als dies für die beabsichtigten Zwecke erforderlich ist. Geht es um die Person selbst, reicht ein Blick auf das Passfoto und den Namen; geht es um die Adresse, reicht ein Blick auf die Rückseite, oder der künftige Arbeitgeber verlangt die Vorlage einer Meldebestätigung. Die Ausweisnummer, der Geburtsort, die Augenfarbe und die Körpergröße sind in der Regel nicht von Belang und die Erhebung und Verarbeitung dieser Daten unzulässig. Bei der Bankkarte verhält es sich ähnlich. Selbstverständlich muss ein Arbeitnehmer eine Bankverbindung angeben, um ihm das Arbeitsentgelt überweisen zu können. Gründe, weshalb die Bankkarte abgelichtet werden sollte, sind nicht ersichtlich. Die Angabe der Kontonummer reicht hierfür völlig aus.
Auch die Einholung der Einwilligung der Betroffenen macht die Anfertigung von Kopien derartiger Dokumente grundsätzlich nicht zulässig. Eine rechtswirksame Einwilligung muss nach § 4 a Abs. 1 Satz Bundesdatenschutzgesetz freiwillig erfolgen. Mit der Freiwilligkeit im Arbeitsverhältnis ist es aber so eine Sache. Von einer freiwillig erteilten Einwilligung kann nur dann ausgegangen werden, wenn dem Beschäftigten eine echte Alternative zur Verfügung steht und er bei deren Inanspruchnahme grundsätzlich keine Nachteile im Arbeitsverhältnis in Kauf nehmen muss.

Arbeitgeber haben keine Befugnis, Kopien von Personalausweisen anzufertigen. Auch die Ablichtung einer Bankkarte ist nicht erforderlich und damit unzulässig. Fordert ein Arbeitgeber hierfür die Einwilligung eines Betroffenen, ist diese regelmäßig unwirksam.

5.3 Coaching und Mitarbeiterüberwachung

Der Betriebsrat eines Call-Centers wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Stellungnahme zu einer Betriebsvereinbarung zum Mitschnitt von Gesprächen zwecks Mitarbeitercoaching und Qualitätsüberwachung.
Bedenken meldete der TLfDI gegen eine vorgesehene von den Betroffenen zu unterzeichnende Einwilligungserklärung zur Durchführung des Mithörens der Telefonate zur Kundenzufriedenheitskontrolle an. Bezeichnend war, dass der Mitarbeiter nach der Bestimmung in der Betriebsvereinbarung seine Tätigkeit nicht ausführen konnte, ohne dass er die Einwilligungserklärung unterzeichnete. Das bedeutet, dass die Einwilligungserklärung nicht, wie nach § 4 a Bundesdatenschutzgesetz (BDSG) gefordert, auf der freiwilligen Entscheidung des Betroffenen beruhte. Die von dieser Vorschrift geforderte Freiwilligkeit ist im Beschäftigtenverhältnis grundsätzlich nicht gegeben. Nur dann, wenn dem Betroffenen eine echte Alternative zur Verfügung steht und ihm durch die Verweigerung der Einwilligung kein Nachteil entsteht, kann von einer rechtswirksamen freiwilligen Einwilligungserklärung ausgegangen werden. Ob im vorliegenden Fall geeignete Alternativen in Form der Beschäftigung an einer anderen Stelle ohne nachteilige Konsequenzen zur Verfügung standen, konnte der TLfDI nicht einschätzen. Bedingt die Einwilligungserklärung jedenfalls, dass der Mitarbeiter überhaupt eine Arbeit ausführen kann, ist nicht von der Freiwilligkeit auszugehen.
Aus den dem TLfDI zur Verfügung gestellten Unterlagen wurde nicht deutlich, ob die Kunden, deren Gespräche von der Zufriedenheits- und Qualitätskontrolle ebenfalls betroffen sind, hiervon erfahren und in welcher Form sie in diese Vorgehensweise einwilligen sollten. Weiteren erheblichen Bedenken begegneten auch das vorgesehene Bewertungs- und Analyseverfahren und in diesem Zusammenhang die Zugriffe durch Vorgesetzte oder andere hierzu berufene Personen auf die Bildschirmarbeit und die Telefontätigkeit. Falls die an einem bestimmten Datum aufgezeichneten Kontakte nicht dem normalen persönlichen Leistungsbild entsprachen, sollten die Beschäftigten nämlich die Möglichkeit haben, außergewöhnliche persönliche Belastungen oder gesundheitliche Gründe anzuführen, um sich zu rechtfertigen. Sofern dies dazu führen würde, dass die Be-

schäftigten aus Angst vor Maßnahmen oder Verlust des Arbeitsplatzes den Datenschutz über Bord werfen und sensible personenbezogene Daten aus dem Privatbereich oder zur Gesundheit offenlegen, entstünde für das Unternehmen ein großes Problem. Diese Daten sind nämlich aus Sicht des TLfDI für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich und könnten daher auch nicht auf der Rechtsgrundlage des § 32 Abs. 1 Satz 1 BDSG erhoben und verarbeitet werden. Auch ein von einem Beschäftigten zur Rechtfertigung seiner Arbeitsleistung zu einem bestimmten Zeitraum vorgelegtes ärztliches Attest dürfte keinesfalls eine Diagnose enthalten. Abgesehen davon, dass die wenigsten Personalverwaltungen über ärztlichen Sachverstand verfügen, wie sollten die Rechtfertigungen eines Beschäftigten für eine Leistung für einen zufällig bestimmten Zeitraum bewertet werden? An der Geeignetheit einer solchen Datenerhebung durch das Unternehmen bestehen daher darüber hinaus ebenfalls erhebliche Zweifel.
Ob die Hinweise des TLfDI letztendlich beim Unternehmen Gehör finden, ist noch offen und wird vom TLfDI beobachtet.

Eine Einwilligungserklärung zur Überwachung und Auswertung von Kundengesprächen zur Zufriedenheitsfeststellung und zum Coaching ist nur auf freiwilliger Basis möglich. Besteht keine echte Alternative im Falle der Ablehnung für die Mitarbeiter, ist die Einwilligung rechtsunwirksam. Damit erfolgt eine Auswertung der Gespräche ohne Rechtsgrundlage. Ein Mitarbeiter kann nicht aufgefordert werden, seine Arbeitsleistung durch Offenbarung sensibler personenbezogener Daten aus seinem Privatbereich oder zu seinem Gesundheitszustand präventiv oder im Nachhinein zu rechtfertigen.

5.4 Fingerabdrücke im Beschäftigtenverhältnis?

Ein in einem Thüringer Unternehmen Beschäftigter bat um Rat im Zusammenhang mit der Arbeits- und Tätigkeitserfassung auf dem ihm vom Arbeitgeber überlassenen Handy, dass über Fingerprint zu aktivieren ist. Der Beschäftigte war an verschiedenen Einsatzorten eingesetzt und sollte seine Arbeitszeiten jeweils an den verschiedenen Standorten mit dem Handy erfassen. Die genaue Handhabung und was der Betroffene genau eingeben sollte, teilte er nicht mit. Ob das Gerät möglicherweise darüber hinaus (Bewegungs-)Daten erfass-

te, ist nicht bekannt. Weitere Informationen zu der eingesetzten Technik gab der Betroffene leider nicht preis.
Arbeitszeiten sind personenbezogene Daten eines Beschäftigten, die auf der Grundlage des § 32 Bundesdatenschutzgesetz (BDSG) für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen. Wie und in welcher Weise die Erfassung erfolgt, ist zunächst freigestellt. Dies kann handschriftlich erfolgen oder in automatisierter Form. Insbesondere bei der automatisierten Erfassung und dem Einsatz technischer Mittel ist die Zweckbindung der Verarbeitung und Nutzung zu beachten. Grundsätzlich gilt, dass eine vollständige Leistungs- und Verhaltenskontrolle mittels automatisierter Verfahren im Beschäftigungsverhältnis auszuschließen ist. Die Feststellung des Aufenthaltsortes des Beschäftigten wäre beispielsweise zulässig, wenn dies für einen Einsatz in Havarie- oder Notfällen notwendig ist. Eine andere Auswertung wäre jedoch auszuschließen.
Will ein Arbeitgeber ein derartiges System zur Arbeitszeiterfassung einsetzen, bedarf es konkreter Festlegungen in einer Betriebsvereinbarung oder einer Betriebsanweisung. Es müssen die Regelungen vorhanden sein, welche konkreten personenbezogenen Daten zu welchem Zweck erfasst werden und wie diese Daten zu welchem Zweck und durch wen ausgewertet werden dürfen. Selbstverständlich müssen die Festlegungen nach dem Grundsatz der Transparenz für die Betroffenen den Beschäftigten auch bekannt sein.
Von der Möglichkeit, dass der TLfDI als Aufsichtsbehörde den Vollzug der datenschutzrechtlichen Vorschriften bei seinem Arbeitgeber im Zusammenhang mit dem Einsatz von Handys zur Erfassung von Arbeitszeit und Standortdaten überprüft, machte er keinen Gebrauch, denn seinen Arbeitgeber nannte er nicht.

Falls der Arbeitgeber beabsichtigt, die Arbeitszeit zukünftig per biometrischer Datenerfassung mittels Fingerabdruck- oder Irisscanner einzuführen, bieten die auf der Homepage des TLfDI veröffentlichten Hinweise zur biometrischen Datenerfassung am Arbeitsplatz weitergehende Informationen.

5.5 Alle Jahre wieder ... Geburtstagslisten

Wie in fast jedem Berichtszeitraum, wurde auch dieses Mal an den Thüringer Landesbeauftragten für den Datenschutz und die Informa-

tionsfreiheit (TLfDI) die Frage herangetragen, ob Geburtstagslisten, diesmal in einem Verein, zulässig seien. Geplagt von Bedenken, wandte sich ein Vorstandsmitglied eines Vereins an den TLfDI, um argumentative Unterstützung in Hinsicht seiner uneinsichtigen Vorstandskollegen zu bekommen. Hierzu erklärte sich der TLfDI gerne bereit. Geburtstagslisten sind datenschutzrechtlich ein alter Hut. Egal, ob es sich um ein Unternehmen oder um einen Verein handelt, es gelten die gleichen Regeln. Geburtstage sind in Verbindung mit einem Namen ein personenbezogenes Datum. Der Umgang mit solchen personenbezogenen Daten wiederum ist nur erlaubt, wenn eine Rechtsvorschrift dies zulässt, dies anordnet oder wenn der Betroffene in den Umgang eingewilligt hat, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Eine Rechtsvorschrift, die eine Geburtstagsliste in einem Unternehmen oder einem Verein zulassen würde, gibt es nicht, weswegen hier nur mit einer Einwilligung gearbeitet werden kann. Dabei muss natürlich darauf geachtet werden, dass die formalen und materiellen Voraussetzungen der Einwilligung eingehalten werden. So muss diese – zumindest im Falle von Geburtstagslisten – schriftlich erfolgen, sie muss freiwillig erklärt werden und es muss sichergestellt sein, dass die einwilligenden Personen ausreichend über die geplante Datenverarbeitung aufgeklärt sind, § 4 a Abs. 1 BDSG.

Geburtstagslisten können in Unternehmen etwas Angenehmes sein. Aber man sollte immer daran denken, dass nicht jeder seinen Geburtstag offen im Intranet oder am schwarzen Brett finden möchte. Solche Listen sind immer nur mit Einwilligung der aufgeführten Mitarbeiter zulässig. Erteilt jemand seine Einwilligung nicht, dann ist diese Person auf der Liste auch nicht zu führen.

5.6 Beratung und Unterstützung von Betriebsräten

Ein weiterer Hilferuf eines Betriebsrats einer Niederlassung eines Unternehmens in Thüringen erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu einer Betriebsvereinbarung, mit der unter anderem die Verarbeitung von Mitarbeiterdaten im Rahmen der Tätigkeit, aber auch die Führung von digitalen Personalakten und die digitale Abrechnung mitbestimmungspflichtig geregelt werden soll.

Die Besonderheit war in diesem Fall, dass die Betriebsvereinbarung zwischen dem Gesamtbetriebsrat und der Geschäftsleitung am Hauptsitz des Unternehmens in einem anderen Bundesland abgeschlossen werden sollte. Anschließend sollte die Betriebsvereinbarung auch für die Niederlassung in Thüringen umgesetzt werden. Ein eigener Datenschutzbeauftragter in der Betriebsstätte in Thüringen war nicht bestellt.
Selbstverständlich kann eine Beratung nur erfolgen, wenn hierfür auch eine Zuständigkeit des TLfDI als Aufsichtsbehörde gegeben ist. Der TLfDI hat nach § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) zwar die Zuständigkeit für Betriebsstätten in Thüringen. Die fragliche Betriebsvereinbarung sollte jedoch in einem anderen Bundesland mit sich später auch entfaltender Wirkung für alle Standorte abgeschlossen werden. Insoweit ist zunächst die am Hauptsitz des Unternehmens zuständige Datenschutzaufsicht zuständig. Nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Im Einvernehmen mit dem Thüringer Betriebsrat wurde daher die Anfrage an die zuständige Datenschutzaufsicht in einem anderen Bundesland abgegeben. Diese hat den TLfDI zwischenzeitlich darüber informiert, von einer Überprüfung der Betriebsvereinbarung werde abgesehen, da der Betriebsrat ihrer Auffassung nach keine verantwortliche Stelle im Sinne des § 38 Abs. 1 Satz 2 BDSG sei und daher kein Anspruch auf Beratung durch die Aufsichtsbehörde bestehe. Gleichwohl ist es aus Sicht des TLfDI vorstellbar, soweit in einer beabsichtigten Betriebsvereinbarung offensichtliche datenschutzschutzrechtliche Mängel erkennbar sind, auch unaufgefordert das Unternehmen selbst zu beraten oder zu kontrollieren.

Wird von einem Unternehmen mit Hauptsitz in einem anderen Bundesland eine Betriebsvereinbarung mit dem Gesamtbetriebsrat abgeschlossen, besteht für den TLfDI keine Zuständigkeit. Betriebsräte sind keine verantwortlichen Stellen im Sinne des § 38 Abs. 1 Satz 2 BDSG und haben daher grundsätzlich keinen Anspruch auf Beratung durch die Datenschutzaufsichtsbehörde. Sollten offensichtliche datenschutzrechtliche Mängel drohen, kann der TLfDI das Unternehmen als verantwortliche Stelle in seinem Zuständigkeitsbereich auch unaufgefordert beraten und kontrollieren.

5.7 Betriebsarzt übermittelt Gesundheitsdaten dem Arbeitgeber

Ein Industrieverband in Thüringen bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) um Beratung zu folgender Frage:
Aufgrund der Vielfältigkeit der Tätigkeitsbereiche werden seitens der Unternehmen so genannte Gefährdungsbeurteilungen für einzelne Arbeitsplätze formuliert. Arbeitnehmer, bei denen es einer gewissen medizinischen und körperlichen Eignung bedarf, werden daher regelmäßig betriebsärztlichen Eignungsuntersuchungen unterzogen, um ihnen gegebenenfalls einen anderen, besser geeigneten Arbeitsplatz zuzuweisen. Dafür müssten die Betriebsärzte den Arbeitgebern Gesundheitsdaten übermitteln. Dabei sollten allerdings keine Diagnosen weitergegeben, sondern nur die Tatsache übermittelt werden, dass der jeweilige Arbeitnehmer für die aktuell ausgeübte Tätigkeit aus medizinischen Gründen „geeignet“ oder „nicht geeignet“ ist. Der Verband wollte wissen, aufgrund welcher Rechtsgrundlage dies möglich sei.
Der TLfDI hat hierzu ausgeführt, dass es sich bei Angaben zu betriebsärztlichen Eignungsuntersuchungen um besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG handele, die einen gesteigerten Schutz genießen. Nach der europäischen Datenschutzrichtlinie ist ihre Verarbeitung nur zugelassen, wenn sie erforderlich ist, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von nationalem Recht, das angemessene Garantien vorsieht, zulässig ist.
Der Arbeitgeber kann nach § 2 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) Betriebsärzte bestellen, wenn dies erforderlich ist im Hinblick auf die Betriebsart und die damit für die Arbeitnehmer verbundenen Unfall- und Gesundheitsgefahren. Die Betriebsärzte haben nach § 3 ASiG Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten.
Hinsichtlich der Durchführung ärztlicher Untersuchungen gilt, dass der Arbeitnehmer aus der allgemeinen Treuepflicht nach § 242 Bürgerliches Gesetzbuch (BGB) verpflichtet sein kann, eine

ärztliche Untersuchung seines Gesundheitszustandes zu dulden. Es müssen jedoch tatsächliche Anhaltspunkte dafür vorliegen, ob und welche Zweifel an der gesundheitlichen Tauglichkeit des Beschäftigten, den Anforderungen des Arbeitsplatzes dauerhaft gerecht zu werden, oder andere sachliche Gründe bestehen, welche die Durchführung einer ärztlichen Untersuchung rechtfertigen (z. B. Versetzung auf einen anderen Arbeitsplatz, für den gesteigerte gesundheitliche Anforderungen bestehen). Aufgrund der besonderen Sensibilität der Daten dürfen weder Diagnosen noch eine vom Arzt ermittelte Anamnese an den Arbeitgeber weitergegeben werden. Es darf lediglich ein allgemeines Urteil über die gesundheitliche Eignung des Mitarbeiters für die konkrete Tätigkeit abgegeben werden.
Die dargestellte beabsichtigte Datenweitergabe seitens des Betriebsarztes an den Arbeitgeber in der Form, ob der jeweilige untersuchte Arbeitnehmer für die aktuell ausgeübte Tätigkeit aus medizinischen Gründen „geeignet“ oder „nicht geeignet“ ist, begegnet keinen datenschutzrechtlichen Bedenken. Es handelt sich dabei um die Verarbeitung personenbezogener Daten des Mitarbeiters nach § 32 Abs. 1 S. 1 BDSG. Einer ausdrücklichen Einwilligung des Arbeitnehmers nach § 4 a Abs. 1 und 3 BDSG (die aufgrund der Freiwilligkeitsproblematik im Beschäftigtenbereich ohnehin problematisch wäre – siehe Nummer 9.10) oder einer entsprechenden Betriebsvereinbarung bedarf es nicht.

Arbeitnehmer können, wenn sie einen Arbeitsplatz innehaben, der eine gesundheitliche Eignung voraussetzt, betriebsärztlich untersucht werden. Der Betriebsarzt darf das Ergebnis der Untersuchung – „geeignet“ oder „nicht geeignet“ – dem Arbeitgeber mitteilen – mehr nicht! Einer Einwilligung des Arbeitnehmers oder einer entsprechenden verpflichtenden Betriebsvereinbarung bedarf es hierzu nicht.

5.8 Chefs mit Kontrollzwang oder Mitarbeiter mit Verfolgungswahn?

Immer wieder wenden sich Beschäftigte Thüringer Unternehmen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie sich intensiven Maßnahmen zur Leistungs- und Verhaltenskontrolle in den Unternehmen ausgesetzt

sehen. Dies geht vom Einsatz von Videokameras über Mithören von Gesprächen oder Telefonaten bis hin zur Fahrzeugortung über GPS.
In einem besonders krassen Fall wurde der dringende Verdacht geäußert, dass alle Mitarbeiterbüros inklusive der Telefonzentrale sowie alle Diensttelefone und Dienstrechner mit Mithörtechnik und/oder Minikameras ausgerüstet sind. Dieser Verdacht gründete sich insbesondere darauf, dass Gesprächsinhalte, die innerhalb des Büros des Betroffenen stattgefunden hatten, plötzlich Gesprächsthema beim Teamleiter waren, obwohl der an den „vertraulichen" Gesprächen überhaupt nicht teilgenommen hatte. Dass das Fahrzeug, das im Außendienst zu nutzen war, mit GPS-Technik oder einer Micro-Kamera mit Tonaufzeichnung ausgerüstet war, wurde ebenfalls vermutet. Die unerklärlichen Dinge gingen soweit, dass der Betroffene sich nach einem privaten Restaurantbesuch unangenehmen Ansprachen des Sicherheitspersonals ausgesetzt sah, er wolle wohl den Arbeitgeber wechseln. Der Beschwerdeführer wurde darauf hingewiesen, es existierten Videos von Geschäftsterminen, an denen auch Vertreter von Wettbewerbsunternehmen teilgenommen hätten.
Dass der Betroffene, wie üblich bei derartigen Nachfragen, anonym bleiben wollte, ist nachzuvollziehen. Der TLfDI kann den Arbeitgeber unter Wahrung der Anonymität des Hinweisgebers auffordern, zu den Vorwürfen der Überwachung der Betriebsstätte und der Fahrzeuge Stellung zu nehmen, um dies datenschutzrechtlich zu überprüfen. Die Wahrung der Anonymität funktioniert aber nur, wenn es sich um einen größeren Mitarbeiterkreis handelt und Einzelheiten keinen Rückschluss auf einen bestimmten Mitarbeiter zulassen. Im vorliegenden Fall informierte der TLfDI den Hinweisgeber wunschgemäß allgemein und wies darauf hin, dass das Mithören und das Aufzeichnen des nicht-öffentlichen gesprochen Wortes eine Straftat darstellen kann. Einem Betroffenen steht in einem derartigen Fall neben einer Beschwerde beim TLfDI auch die Möglichkeit einer Strafanzeige bei der Staatsanwaltschaft offen.

Besteht der Verdacht, dass in einem Unternehmen das nicht-öffentlich gesprochene Wort abgehört wird, kann der hiervon Betroffene auch wegen einer Straftat nach § 201 Strafgesetzbuch (StGB) bei der Staatsanwaltschaft oder der Polizei Strafantrag stellen.

5.9 Die Suche nach Personalakten

Nachdem das Arbeitsverhältnis Anfang 2014 beendet war, wollte eine Arbeitnehmerin von ihrem ehemaligen Arbeitgeber ihre Steuerunterlagen zurück. Aufgrund verschiedener widersprüchlicher Angaben ihres Arbeitgebers wandte sie sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie letztendlich davon ausging, dass ihre Personalakte bereits kurz nach der Beendigung des Arbeitsverhältnisses vernichtet worden war.

Auf Nachfrage teilte das Unternehmen mit, die Arbeitnehmerin habe die Steuerkarte zurückgefordert. Es könne keine Steuerkarte zurückgegeben werden, weil seit dem Jahr 2010 keine Lohnsteuerkarten mehr ausgegeben werden und seither alle steuerrechtlichen Belange über die Steueridentifikationsnummer abgewickelt werden. Die Steueridentifikationsnummer werde nach Mitteilung durch die Arbeitnehmer lediglich auf dem Personalbogen notiert. Der Personalbogen werde jedoch nicht herausgegeben. Es wurde durch das Unternehmen ausgeschlossen, dass Personalunterlagen, auf denen sich alle notwendigen Angaben zur Abrechnung befanden, vernichtet worden seien. Anlässlich der Überprüfung der Unterlagen hatte sich jedoch herausgestellt, dass in der Tat der Arbeitsvertrag mit der Betroffenen im Unternehmen nicht auffindbar war.

Diese Einlassung veranlasste den TLfDI zur Überprüfung der internen Festlegungen zum Umgang mit Personalunterlagen. Die dargelegten Festlegungen und Vorgehensweisen in dem Unternehmen begegneten keinen datenschutzrechtlichen Bedenken. Personaldokumente wie Bewerbungsunterlagen, der Arbeitsvertrag und der ausgefüllte Personalbogen wurden in einer Personalakte zu dem Betroffenen abgeheftet. Zugang haben nur die zuständigen Mitarbeiter der Personalverwaltung. Nach Beendigung des Arbeitsverhältnisses werden die Dokumente nach den Vorgaben des Bürgerlichen Gesetzbuchs, der Abgabenordnung und den sozialgesetzlichen Vorschriften aufbewahrt. Weshalb der Arbeitsvertrag nicht mehr vorhanden war, konnte allerdings intern nicht mehr geklärt werden. Hinweise darauf, dass er in unbefugte Hände geraten wäre, gab es auch nicht.

Auch wenn der Arbeitsvertrag aus nicht mehr nachvollziehbaren Gründen nicht mehr auffindbar war, war dennoch sichergestellt, dass die notwendigen Angaben für Prüfungs- und Rechnungszwecke

vorhanden sind. Damit konnte gegebenenfalls auch Auskunftsbegehren der Betroffenen auch nach dem Ausscheiden aus dem Unternehmen nachgekommen werden.
Der Betroffenen hat der TLfDI mitgeteilt, die Befürchtung, ihre Personalakte sei bereits vernichtet worden, habe sich nicht bestätigt. Auch wenn sich der Arbeitsvertrag aus unerfindlichen Gründen nicht bei den Personaldokumenten befindet, seien nach Darlegung des ehemaligen Arbeitgebers die für eventuelle Auskünfte erforderlichen Unterlagen und die nach gesetzlichen Vorschriften aufzubewahrenden Unterlagen für Nachweis und Prüfungszwecke vorhanden. Im Übrigen gebe es nach Beendigung des Arbeitsverhältnisses grundsätzlich keinen Herausgabeanspruch zu einzelnen Unterlagen aus der Personalakte.

Arbeitnehmer haben nach Beendigung des Arbeitsverhältnisses grundsätzlich keinen Anspruch gegen den ehemaligen Arbeitgeber auf Herausgabe ihrer Personalakte oder einzelner Unterlagen. Mangels konkreter Bestimmungen zum Inhalt von Personalakten im Unternehmen kann sich eine Personalakte auf wenige Unterlagen beschränken, die für Rechnungslegungs- und Prüfzwecke (durch Fiskus, Rentenversicherung, Krankenkasse etc.) erforderlich sind.

5.10 Arbeitgeber will den Mutterpass sehen

Eine Arbeitnehmerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Unterstützung. Hintergrund war, dass sie ihren Arbeitgeber über ihre Schwangerschaft in Kenntnis gesetzt hatte. Gleichzeitig händigte sie dem Arbeitgeber ein ärztliches Schwangerschaftsattest mit allen relevanten Daten (voraussichtlicher Entbindungstermin, aktuelle Schwangerschaftswoche, letzter Arbeitstag vor dem Beschäftigungsverbot nach dem Mutterschutzgesetz) aus. Der Arbeitgeber wollte aber die Schwangerschaft nicht anerkennen, da die Betroffene nicht bereit war, ihren Mutterpass vorzulegen und kopieren zu lassen.
Der Betroffenen wurde folgende rechtliche Einschätzung des TLfDI mitgeteilt:
Das Erstellen einer Kopie des Mutterpasses erfüllt den Tatbestand des Erhebens personenbezogener Daten durch den Arbeitgeber. Dies ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur zulässig,

wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da eine Einwilligung nicht vorlag und es im Übrigen wegen des bestehenden Beschäftigungsverhältnisses auch an deren Freiwilligkeit fehlen würde, muss eine Rechtsvorschrift das Erheben dieser Daten erlauben. Sofern eine spezielle Ermächtigungsgrundlage nicht existiert, ist das Erheben von Beschäftigtendaten nach § 32 BDSG nur zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Nach § 5 des Mutterschutzgesetzes sollen werdende Mütter dem Arbeitgeber ihre Schwangerschaft und den mutmaßlichen Tag der Entbindung mitteilen, sobald ihnen ihr Zustand bekannt ist. Auf Verlangen des Arbeitgebers sollen sie das Zeugnis eines Arztes oder einer Hebamme vorlegen. Aufgrund der für Schwangere geltenden besonderen gesetzlichen Bestimmungen ist die Kenntnis von der Schwangerschaft und des voraussichtlichen Entbindungstermins für die Durchführung des Beschäftigungsverhältnisses für den Arbeitgeber in aller Regel erforderlich. Nicht erforderlich ist aber das Erheben der im Mutterpass zusätzlich zu diesen Angaben enthaltenen personenbezogenen Daten. Der Mutterpass enthält Informationen über die Gesundheit der Schwangeren, unter anderem Ergebnisse von Laboruntersuchungen, Angaben dazu, ob eine Rötelnerkrankung vorlag, ob die Schwangere mit Chlamydien – einer bestimmten Art von Bakterien – infiziert ist, ob eine HIV-Infektion besteht, ob eine Infektion mit Syphilis-Erregern nachgewiesen wurde, ob eine Erkrankung an Hepatitis B besteht und vieles mehr.
Der Arbeitgeber durfte daher im vorliegenden Fall die Vorlage des Mutterpasses nicht verlangen. Der Beschwerdeführerin wurde mitgeteilt, dass, sollte er gleichwohl eine Kopie des Mutterpasses fertigen, die Einleitung eines Ordnungswidrigkeitenverfahrens zu prüfen wäre. Nach § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt. Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 300.000 Euro geahndet werden. Der Betroffenen wurde geraten, dem Arbeitgeber das Schreiben des TLfDI zur Kenntnis vorlegen. Die Beschwerdeführerin hat sich daraufhin nicht mehr gemeldet.

Die Kenntnis von der Schwangerschaft und des voraussichtlichen Entbindungstermins für die Durchführung des Beschäftigungsverhältnisses ist für den Arbeitgeber in aller Regel erforderlich. Nicht erforderlich und damit unzulässig ist aber das Erheben der im Mutterpass zusätzlich zu diesen Angaben enthaltenen personenbezogenen Daten.

5.11 Nur weil's einer wissen darf, heißt es noch lange nicht, dass es ein anderer erzählen darf.

Ein Verein, der Aufträge von Einzelpersonen an bei ihm gelistete Mitgliedsunternehmen vermittelt, änderte im Berichtszeitraum seine Satzung. Mit dieser Änderung sollten die Mitgliedsunternehmen verpflichtet werden, dem Verein gegenüber durch Übersendung von Arbeitsverträgen ihrer Arbeitnehmer bestimmte Standards nachzuweisen. Konkret ging es dem Verein um die fachliche Qualifikation der Mitarbeiter. Sollten die entsprechenden Standards nicht gegeben sein oder die Arbeitsverträge nicht übersandt werden, so würden an das jeweilige Mitgliedsunternehmen keinerlei Aufträge mehr vermittelt.
Mit diesem Sachverhalt meldete sich ein Unternehmen aus Hessen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Man habe, so wurde es von diesem Unternehmen mitgeteilt, Zweifel an der Zulässigkeit des Vorgehens des thüringischen Vereins.
Diese Zweifel konnte der TLfDI nur bestätigen. Datenschutzrechtlich ist dieser Fall im Übrigen sehr geeignet, die immerwährende eigene Verantwortung als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetz (BDSG) aufzuzeigen. Denn: Der Verein darf die geforderten Daten soweit vom TLfDI geprüft, tatsächlich erheben. Das Perfide ist: Seine Mitgliedsunternehmen dürfen sie nicht an den Verein übermitteln. Und zwar unter keinen Umständen. Das BDSG ist an dieser Stelle eindeutig. Personenbezogene Daten dürfen nur dann erhoben, verarbeitet oder genutzt werden, wenn ein Gesetz dies erlaubt oder anordnet oder der Betroffene in den jeweiligen Umgang mit seinen personenbezogenen Daten eingewilligt hat, § 4 Abs. 1 BDSG. Der Begriff der Übermittlung fällt unter den Begriff der Verarbeitung.
Verantwortliche Stelle ist zunächst einmal das Mitgliedsunternehmen als Arbeitgeber des jeweils angeforderten Arbeitsvertrages. Und

diese Arbeitnehmerdaten dürfen nach § 32 Abs. 1 Satz 1 BDSG nur dann übermittelt werden, wenn es für die Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Dies ist nicht der Fall. Damit ist die Übermittlung unzulässig.
Häufig entstehen Datenschutzverstöße dadurch, dass davon ausgegangen wird, eine Befugnis zur Datenerhebung würde – automatisch – mit einer Befugnis zur Datenübermittlung an die erhebende Stelle korrelieren. Nach dem Motto: Wenn die Stelle Daten erheben darf, darf ich die Daten auch an sie übermitteln. Dem ist indes nicht so. Für jeden Abschnitt der Datenverarbeitung – also Erhebung, Speicherung, Übermittlung, Löschung, Sperrung – ist eine eigene Befugnisnorm bzw. Einwilligung erforderlich.

Verantwortliche Stellen, also Unternehmen und Personen, die personenbezogene Daten erheben und verarbeiten, sind immer gut beraten, ihre Kompetenzen beim Umgang mit diesen zu prüfen. Fordert ein Dritter Informationen an, heißt das noch lange nicht, dass die verantwortliche Stelle diese Informationen tatsächlich herausgeben darf. Passiert dies dennoch und es liegt keine Übermittlungsbefugnis vor, drohen Verwaltungsverfahren und/oder Bußgeldverfahren von Seiten des TLfDI.

5.12 Unfallanzeige an die Berufsgenossenschaft

Unter welchen Voraussetzungen eine externe Fachkraft für Arbeitssicherheit (Sicherheitsfachkraft) in ihren Kundenbetrieben denn eine Unfallanzeige für die Berufsgenossenschaft erstellen dürfe, fragte ein hiermit Beauftragter den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil mit einer derartigen Anzeige natürlich auch immer die Übermittlung personenbezogener Daten verbunden ist.
Der TLfDI verwies zunächst auf die gesetzlichen Regelungen. Gemäß § 193 Abs. 1 Sozialgesetzbuch (SGB) Siebtes Buch (VII) hat ein Unternehmer Unfälle von Versicherten in seinem Unternehmen dem Unfallversicherungsträger anzuzeigen. Der Unternehmer muss die Pflicht jedoch nicht in eigener Person erbringen, sondern er kann eine andere Person mit der Übernahme dieser Pflicht beauftragen. Dass diese Person zwingend dem Unternehmen angehören muss, ist den Regelungen nicht zu entnehmen.

Nach § 193 Abs. 5 SGB VII ist die Anzeige vom Betriebs- oder Personalrat mit zu unterzeichnen. Darüber hinaus hat der Unternehmer die Sicherheitsfachkraft und den Betriebsarzt des Unternehmens über jede Unfall- oder Berufskrankheitsanzeige in Kenntnis zu setzen. Da also auch die Sicherheitsfachkraft von der Anzeige in Kenntnis zu setzen ist, erhält sie damit auch die erforderlichen Personaldaten des vom Unfall Betroffenen. Daher ist es nach Auffassung des TLfDI unbedenklich, wenn eine externe Fachkraft für Arbeitssicherheit die Anzeige erstellt, die sie ohnehin selbst auch erhalten würde.
Die Verarbeitung der Daten durch das Unternehmen richtet sich nach den allgemeinen Vorschriften des Bundesdatenschutzgesetzes (BDSG) und nicht nach dem SGB. Um Sozialdaten handelt es sich nur, wenn die personenbezogenen Daten durch eine Stelle nach dem SGB verarbeitet werden. Damit unterfallen diese Daten im Unternehmen nicht dem Sozialgeheimnis gemäß § 35 SGB I. Mit der Beauftragung eines Externen als Sicherheitsfachkraft sind die erforderlichen Regelungen im Rahmen der Auftragsdatenverarbeitung nach § 11 BDSG zu treffen. Selbstverständlich ist eine externe Fachkraft auch auf das Datengeheimnis nach § 5 BDSG zu verpflichten. Unter diesen Bedingungen kann also auch eine externe Sicherheitsfachkraft damit beauftragt werden, eine Unfallanzeige anzufertigen.

Ein Unternehmer muss eine Unfallanzeige nicht in eigener Person erbringen. Diese Pflicht kann er auch auf eine Sicherheitsfachkraft außerhalb des Unternehmens delegieren, weil diese Person ohnehin über einen Unfall zu informieren ist.

5.13 Wie heißt die Schwester? – Namensschilder im Krankenhaus

Mit gewisser Regelmäßigkeit wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gefragt, ob Beschäftigte denn verpflichtet seien, ein Namenschild mit Vor- und Nachnamen zu tragen, weil der Arbeitgeber dies als besonderen Service zur Ansprechbarkeit betrachtet. Das Krankenhauspersonal insbesondere im Pflegebereich hat allerdings meistens etwas dagegen, den vollen Namen zur Schau zu tragen. Nach Feierabend möchte man ungern von Patienten kontaktiert werden, die in der Pflege-

leistung in der Klinik womöglich mehr gesehen haben als die Dienstverrichtung.
Bei dem Namen eines Beschäftigten handelt es sich um ein personenbezogenes Datum, jedoch ist der Name als solcher nicht schon aus dem Grund, dass er in der Personalakte enthalten ist, ein besonders sensibles personenbezogenes Beschäftigtendatum. Das Tragen eines Namensschildes während der Arbeit stellt einen Vorgang dar, dessen Zulässigkeit sich nach § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) beurteilt. Da der Name zum Zweck der Kenntnis Dritter getragen werden soll, handelt es sich um eine Datenübermittlung. Dies begegnet keinen datenschutzrechtlichen Bedenken, wenn ein berechtigtes Interesse des Arbeitgebers als der verantwortlichen Stelle an dem Tragen der Namensschilder besteht und keine schutzwürdigen Interessen der Beschäftigten am Schutz ihrer Privatsphäre überwiegen. Die Persönlichkeitsrechte der Beschäftigten können dann beeinträchtigt werden, wenn in einem Krankenhaus Patientenkontakt besteht und die Beschäftigten verpflichtet werden, das Namensschild mit Vor- und Nachnamen zu tragen. Oftmals wird von den Betroffenen befürchtet, dass ihre Namen anhand öffentlicher Telefonbücher oder über eine Suchmaschine im Internet mit der Privatanschrift verbunden werden können und sie damit für Patienten auch im Privatleben ansprechbar werden. Dies sind gewichtige Aspekte, die die Interessensabwägung zugunsten des Pflegepersonals ausfallen lassen. Insoweit muss der Arbeitgeber es den Beschäftigten freistellen, ob der vollständige oder der Nachname oder, wie in Krankenhäusern für das Pflegepersonal üblich, nur der Vorname auf dem Namensschild angebracht wird.

Bei Klinikpersonal im Pflegebereich reicht grundsätzlich die Angabe der Funktion und des Vornamens zur Ansprechbarkeit für Patienten aus. Das Pflegepersonal darf nicht gezwungen sein, zusätzlich auch den Nachnamen auf dem Namenschild zu tragen. Die Interessensabwägung zum Schutz der Betroffenen fällt regelmäßig zu deren Gunsten aus, wenn Nachstellungen im Privatleben nicht auszuschließen sind.

5.14 Seminarteilnehmer per E-Mail anschreiben: Was ist zu beachten?

Der Mitarbeiter eines Unternehmens, das Fortbildungen anbot, fragte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob es denn rechtlich geregelt sei, ob er über die E-Mail-Adresse eines anderen Unternehmens Teilnehmer an Seminaren anschreiben dürfe. Nach seinem Dafürhalten übermittele er doch auf diese Weise keine personenbezogenen Daten der Teilnehmer.
Da die näheren Umstände vom Fragesteller trotz Rückfrage des TLfDI nicht dargelegt wurden (z. B.: Weshalb soll diese E-Mail-Adresse genutzt werden? Wurde die Fortbildung vom Unternehmen, das die E-Mail-Adresse besitzt, selbst veranlasst oder genehmigt oder ist der Fragesteller selbst in beiden Unternehmen tätig?), hat der TLfDI nur allgemein ausgeführt, eine konkrete gesetzliche Regelung hierzu gäbe es nicht.
Die Nutzung von E-Mail-Adressen eines Unternehmens wird üblicherweise durch eine Betriebsvereinbarung oder Anweisung in dem Betrieb, dem die E-Mail-Adresse zuzuordnen ist, geregelt. Es kommt darauf an, ob die E-Mail-Adresse des Unternehmens, auch wenn diese durch die Nennung des Mitarbeiters Personenbezug aufweist, nur für Unternehmenszwecke oder auch für andere Zwecke genutzt werden darf. Dem Unternehmen ist in der zugrundeliegenden Vereinbarung oder Anweisung in der Regel eine Kontrollbefugnis zu den ein- und ausgehenden E-Mails eingeräumt. Selbst wenn nur der Header für Kontrollzwecke genutzt wird, käme dem Unternehmen bzw. der zur Kontrolle befugten Person zur Kenntnis, wer Seminarteilnehmer ist oder war. Je nachdem, ob dies gewollt ist oder vermieden werden soll, ist zu entscheiden, auf welchem Weg Seminarteilnehmer angeschrieben werden. Hat das in der E-Mail-Adresse bezeichnete Unternehmen mit dem Seminar selbst nichts zu tun, dürfen ihm auch die Seminarteilnehmer nicht zur Kenntnis gelangen, weil ihm keine eigenen Erhebungsbefugnisse nach § 28 Bundesdatenschutzgesetz (BDSG) bzw. bei eigenen Mitarbeitern nach § 32 BDSG zukommen.
Der Fragesteller bedankte sich beim TLfDI für die Ausführungen, die er für hilfreich erachtete.

Bevor die E-Mail-Adresse eines Unternehmens genutzt wird, muss man sich kundig machen, welche Regelungen intern zur Nutzung getroffen sind. Bestehen Kontrollbefugnisse zu ein- und ausgehenden E-Mails, sollte der Versender von E-Mails darauf achten, dass dem Unternehmen keine personenbezogene Daten offenbart werden, die dieses nicht erheben darf.

5.15 Der gläserne Kraftfahrer

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) prüfte ein größeres Logistikunternehmen, das in den LKW seines Fuhrparks ein Global Positioning System (GPS) betrieb. Eine Einwilligung der Kraftfahrer für die Erhebung, Verarbeitung, Nutzung und Archivierung ihrer Daten mittels des GPS-Überwachungssystems war nicht vorhanden. Weiterhin diente das GPS-System auch der Disposition des Logistikunternehmens. Darüber hinaus erfasste das System alle personenbezogenen Daten der persönlichen Fahrerkarte. In dieser Überwachung sah der Betriebsrat eine Überwachung der Arbeitsleistung und des Arbeitsverhaltens. Vor allem erfolge die Überwachung nicht nur während der Arbeits- und Bereitschaftszeiten, sondern auch in den Pausen bzw. der Freizeit. Daraufhin führte der TLfDI eine Vorortkontrolle auf dem Betriebsgelände durch. Dabei wurde festgestellt, dass es in dem Logistikunternehmen keine Betriebsvereinbarung zur Nutzung eines derartigen Systems gab.
Das GPS-System ist aus datenschutzrechtlicher Hinsicht nicht unproblematisch. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des Bundesdatenschutzgesetzes oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Daher ist auch der Einsatz von Ortungstechnik, sobald damit die Ortung von Personen, hier Beschäftigten, verbunden ist, einem grundsätzlichen Verbot unterworfen, weil hierdurch Bewegungs- und Verhaltensdaten erhoben werden, die personenbezogene Daten darstellen. Auch dürfen Beschäftigte keineswegs einem permanenten Kontrolldruck ausgesetzt sein. Als mögliche Erlaubnisnormen kamen für die mittels GPS erfolgende Erhebung und Verarbeitung personenbezogener Daten die §§ 28 Abs. 1 Satz 1 Nr. 2 und 32 Abs. 1 Satz 1 BDSG in Betracht. Ohne eine den datenschutz-

rechtlichen Erfordernissen genügende Einwilligung, wie auch in diesem Fall, kann die mittels GPS erfolgende Verarbeitung personenbezogener Daten nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein, soweit sie für die Erfüllung eigener Geschäftszwecke erfolgt, zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der oder des Beschäftigten am Ausschluss der Verarbeitung oder Nutzung überwiegt.

Im Einzelnen kommt es auf den Zweck der Datenverarbeitung, die technischen Möglichkeiten des Systems und dessen tatsächlichen Gebrauch an. So wäre es datenschutzrechtlich unproblematisch, wenn die Ortung durch das System technisch etwa erst nach einem Kfz-Diebstahl einsetzen würde. Der Ortung von Gegenständen dienende Zwecke (z. B. die Warenverfolgung des Fuhrparks), die offensichtlich im berechtigten Interesse des Unternehmens liegen, sind grundsätzlich nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig. Soweit dabei zugleich Daten des Fahrpersonals gespeichert werden, sind die im Folgenden beschriebenen Regelungen über den Umgang mit diesen Daten zu beachten. Auswertungsfunktionalitäten, die nur der allgemeinen persönlichen Überwachung von Beschäftigten dienen können (wie etwa Geschwindigkeitsaufzeichnungen, Dauer von Fahrtunterbrechungen), sind regelmäßig technisch zu unterbinden. Ein System zum Beispiel, das über eine Alarmierungsfunktion verfügt, die die Arbeitgeberin oder den Arbeitgeber informiert, wenn Beschäftigte eine definierte Zone verlassen oder sich zu lange in einer solchen aufhalten, würde einen permanenten Kontrolldruck erzeugen. Es ist deswegen nicht zulässig.

Der Einsatz von Ortungstechnik, die der gezielten Überwachung des Verhaltens von Arbeitnehmerinnen und Arbeitnehmern dient, kommt nur in ganz begründeten Einzelfällen in Betracht. Kontrollen sind nur unter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig. Demgemäß müssen Beschäftigte Kontrollen ihres Arbeitsverhaltens nur dann hinnehmen, wenn diese geeignet und erforderlich sind, um etwa konkreten Verdachtsmomenten auf arbeitsrechtliche Verfehlungen nachzugehen. Es müssen tatsächliche Anhaltspunkte bestehen, die den Verdacht rechtfertigen, dass die überwachten Personen gegen ihre arbeitsrechtlichen Pflichten verstoßen (§ 32 Abs. 1 BDSG).

Nicht nur bei einer gezielten Überwachung von Beschäftigten im Verdachtsfall, sondern auch, wenn bei einer Ortung von Gegenstän-

den personenbezogene Daten anfallen, muss der Umgang mit diesen Daten in einer Betriebsvereinbarung klar geregelt sein. Deswegen müssen folgende Punkte beachtet werden:
Da die Nutzung der personenbezogenen Daten nur zulässig ist, soweit dies im Rahmen der oben beschriebenen Interessenabwägung erforderlich ist, wird in einer Betriebsvereinbarung zu regeln sein, welche Daten konkret erhoben werden. Die Einzeldaten müssen unter Nennung des gesetzlich bestimmten Zwecks aufgeführt werden (z. B. „zwecks steuerlicher Anerkennung des betrieblichen Einsatzes: Datum, Fahrstrecke, Ort der Auftragserfüllung“). Die Speicherfrist ist unter Abwägung der betrieblichen Erfordernisse und der Datenschutzinteressen der betroffenen Beschäftigten konkret mit möglichst kurzer Aufbewahrungsdauer festzulegen.
In der Betriebsvereinbarung muss verdeutlicht werden, dass eine permanente und allgemeine Verhaltens- oder Leistungskontrolle aus datenschutz- sowie arbeitsrechtlichen Gründen unzulässig und vom Direktionsrecht der Unternehmensleitung nicht umfasst ist. Zulässig sind Stichproben sowie durch einen begründeten Verdacht veranlasste Kontrollen. Es sollte auch klargestellt werden, dass arbeitsrechtliche Maßnahmen gemäß § 6a Abs. 1 BDSG nicht ausschließlich aufgrund von Informationen ergriffen werden dürfen, die auf GPS-gestützten Datenerfassungen beruhen.
Im Ergebnis erstellte das Logistikunternehmen eine entsprechende Betriebsvereinbarung. Ob diese den vorgenannten Punkten entspricht, wird derzeit noch vom TLfDI überprüft. Über den Ausgang des Verwaltungsverfahrens wird im nächsten Tätigkeitsbericht informiert werden.

Nach dem datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG) ist der Einsatz von GPS-Systemen nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder eine wirksame Einwilligung des Betroffenen gemäß § 4a BDSG vorliegt. Rechtsgrundlage für einen konformen Einsatz dürfte in den meisten Fällen § 28 Abs. 1 Nr. 2 BDSG bzw. § 32 Abs. 1 BDSG sein. Hiernach sind die berechtigten Interessen des Unternehmens als datenverarbeitende Stelle gegen schutzwürdige Interessen des von der Tracking-Maßnahme Betroffenen abzuwägen. Bei allen Fällen, die eine GPS-Ortung von Außendienstmitarbeitern rechtfertigen, ist grundsätzlich zu beachten, dass die jeweilige Datenverarbeitung streng zweckgebunden erfolgen

muss. Für einen bestimmten Zweck erhobene und gespeicherte Daten dürfen nicht für einen anderen genutzt werden.

5.16 Von Räuberpistolen – Datenschutz im Logistikunternehmen

Von A bis Z, von der Angel bis zur Zahnbürste, alles kann bei den großen Händlern im Internet bestellt werden und ist in der Regel schon am nächsten Tag bei einem zu Hause. Ein Komfort, der einen oft vergessen lässt, welch organisatorischer Aufwand hinter diesem Prozess steht, der diese Schnelligkeit bei gleichzeitiger Warenfülle gewährleistet. Wie geht das, fragen Sie sich? Nun, kurz und ohne Umschweife: Daten, Daten und nochmals Daten. Nicht alle personenbezogen, aber letztlich doch viele.
Die Lager der Händler sind in der Regel chaotisch sortiert. Darunter versteht man eine Lagerhaltung, die zwar sehr effektiv, aber ohne Computer nicht zu handhaben ist. Natürlich gibt es eine gewisse Grundordnung, letztlich werden aber einzulagernde Waren dort aufbewahrt, wo Platz ist und nicht unbedingt dort, wo ähnliche oder dazugehörige Teile gelagert werden. Wegen der vielen unterschiedlichen Formen der Waren müssen diese jedoch von Menschen einsortiert werden. Jede dieser Personen hat eine Scan-Pistole. Über diese wird der Einlagerungsprozess gesteuert und dokumentiert. Allerdings lässt sich über die damit erhobenen Daten nicht nur der Lagerort der Ware bestimmen, sondern auch recht genau die Arbeitsleistung des Pistoleros.
Ein solches Logistiklager hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum geprüft. Das Verfahren ist, auch wegen der umfangreichen IT des Unternehmens, noch nicht ganz abgeschlossen, befindet sich aber auf einem guten Weg. Aus Sicht das Datenschutzes, also aus Sicht des TLfDI ist problematisch, dass einerseits das Unternehmen die erhobenen Daten über die Waren- und Logistikprozesse unbedingt benötigt, andererseits aber irgendwie sichergestellt werden muss, dass dabei keine Arbeitnehmerdaten erhoben oder verarbeitet werden, die nicht hätten erhoben oder verarbeitet werden dürfen. Das Gesetz verlangt von der verantwortlichen Stelle hierfür technische und/oder organisatorische Maßnahmen (sog. Technische und organisatorische Maßnahmen oder kurz TOMs), die dies verhindern. Das Unternehmen arbeitet kooperativ mit dem TLfDI an einer Lösung.

Verantwortliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um das Bundesdatenschutzgesetz umzusetzen.

5.17 Bei Anruf Chef! – Nachprüfung der Dienstreisezeiten im Hotel

Wie würden Sie das finden, wenn Ihr Arbeitgeber im Nachgang kontrolliert, zu welcher Zeit Sie das Hotel während einer Dienstreise verlassen haben? Im Berichtszeitraum informierte ein Arbeitnehmer einer Firma den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), dass die Mitarbeiter des Hotels, in welchem sich dieser während seiner Dienstreise aufhielt, seinem Arbeitgeber einfach Ankunfts- und Abreisezeiten telefonisch preisgaben.
Der Arbeitgeber hatte im Nachgang der Dienstreise seines Arbeitnehmers telefonisch Informationen zu dem Hotelaufenthalt seines Mitarbeiters eingeholt. Ohne sich eines datenschutzrechtlichen Verstoßes bewusst zu sein, nannte ein Mitarbeiter des Hotels dem Arbeitgeber die Check-Out-Zeit. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Übermittlung personenbezogener Daten – hier vom Hotel zum Arbeitgeber – nur zulässig, soweit es das BDSG oder eine andere Rechtsvorschrift erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Einwilligung des Arbeitnehmers lag nicht vor. Schließlich ist das Übermitteln der Ankunfts- und Abreisezeiten an den Arbeitgeber durch das Hotel auch nicht von der im vorliegenden Fall in Betracht kommenden Erlaubnisnorm des § 28 Abs. 1 BDSG gedeckt. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Verarbeiten und damit folglich das Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel eigener Geschäftszwecke zulässig, wenn es für die Begründung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen, also dem, auf den sich die Daten beziehen, erforderlich ist. Vorliegend war die Erhebung der Ankunfts- und Abreisezeiten des Arbeitnehmers nur für die Begründung des Beherbergungsvertrages zwischen dem Hotel und dem Hotelgast, dem Arbeitnehmer und somit zur Erfüllung eigener Geschäftszwecke erforderlich, nicht aber für den Arbeitgeber.

Nach § 28 Abs. 1 Nr. 2 und Nr. 3 BDSG ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Nr. 2), oder wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der verantwortlichen Stelle offensichtlich überwiegt (Nr. 3).
Bei den Ankunfts- und Abreisezeiten des Arbeitnehmers im Hotel handelt es sich nicht um allgemein zugängliche Daten im Sinne des BDSG. Sie werden lediglich im Rahmen automatisierter Verarbeitungen durch das Hotel bzw. in nicht automatisierten Dateien des Hotels für eigene Geschäftszwecke vorgehalten.
Zwar mag der Arbeitgeber unter Umständen ein berechtigtes Interesse an diesen Informationen haben, jedoch überwiegt im Ergebnis nach Prüfung durch den TLfDI das schutzwürdige Interesse des Arbeitnehmers. Vor allem im Hinblick auf arbeitsrechtliche Konsequenzen muss dies auch für den Hotelier offensichtlich sein.
Der TLfDI hat das Hotel über die Rechtslage aufgeklärt, woraufhin Mitarbeiterschulungen durch den Hotelier veranlasst wurden.

Zwar mag der Arbeitgeber personenbezogene Daten seiner Arbeitnehmer nach § 32 Abs. 1 BDSG erheben dürfen, so auch Ankunftszeiten in einem Hotel, jedoch darf das Hotel selber, als eigene verantwortliche Stelle, diese nicht an den Arbeitgeber übermitteln, es sei denn, der Arbeitnehmer willigt ein. Ein Erlaubnistatbestand, der dies zulassen würde, existiert nicht. Vermutet der Arbeitgeber einen Arbeitszeitbetrug, bleibt ihm nur der Weg über die Ermittlungsbehörden.

5.18 Bewerbung per E-Mail?

Ein Bewerber auf einen Arbeitsplatz in einem Unternehmen fragte, ob es denn in Ordnung sei, dass er in der Bewerbungsphase mit einem Mitarbeiter über dessen erkennbar private E-Mail-Adresse kommunizieren sollte.

Hierzu hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) allgemein ausgeführt, dass die Nutzung von E-Mail in Unternehmen in der Regel nach den dortigen Betriebsvereinbarungen oder
-anweisungen unter Berücksichtigung der Regelung des § 9 Bundesdatenschutzgesetz zu beurteilen ist. Danach haben nicht-öffentliche Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung datenschutzrechtlicher Vorschriften zu gewährleisten. Jedoch wäre es unzulässig, wenn vom Unternehmen festgelegt wäre, dass im Bewerbungsverfahren über die privaten E-Mailadressen von Mitarbeitern mit potenziellen Arbeitskräften kommuniziert werden darf.
Im Hinblick auf die datenschutzrechtlichen Belange insbesondere zur Vertraulichkeit der Kommunikation, die im E-Mail-Verkehr bekanntlich äußerst fraglich ist, müssten in einem solchen Fall seitens des Unternehmens geeignete Sicherheitsmaßnahmen getroffen werden. Da es sich bei Bewerberdaten wie beispielsweise Schulabschlusszeugnissen, Arbeitszeugnissen, Lebensläufen etc. um schützenswerte personenbezogene Daten handelt, wäre durch geeignete Maßnahmen sicherzustellen, dass die Bewerbung ohne Kenntnis Unbefugter zumindest innerhalb des Unternehmens den zuständigen Mitarbeiter erreicht. Daher sollte geeignete Verschlüsselungstechnik eingesetzt werden.
Das Angebot des TLfDI, der Sache weiter nachzugehen, hat der Betroffene nicht angenommen.

Werden Bewerbungen per E-Mail verschickt, muss sich der Versender darüber klar sein, dass die Vertraulichkeit nur dann gewahrt werden kann, wenn zusätzliche Sicherheitsmaßnahmen zum Schutz vor der Kenntnisnahme Unbefugter getroffen sind. Es sollte unbedingt eine Verschlüsselungstechnik eingesetzt werden. Nur unter diesen Voraussetzungen sollten Unternehmen mit Bewerbern via E-Mail kommunizieren.

5.19 Mitarbeiterüberwachung durch Handscanner?

Anlässlich der Durchführung einer datenschutzrechtlichen Kontrolle der Videoüberwachung in einem Logistikunternehmen wurde festgestellt, dass dort so genannte Handscanner genutzt werden. Diese

Geräte erlauben die Speicherung von Mitarbeiterdaten dazu, wer wann welches Produkt wohin verbracht hat.
Das Handgerät verfügt über eine Windowsoberfläche und kann grundsätzlich alles, was ein PC auch kann. In dem Logistikunternehmen wird der Wareneingang und -ausgang registriert. Somit ist jeweils nachvollziehbar, wann sich welches Warenteil wo befindet, aber auch, welcher Mitarbeiter zu welchem Zeitpunkt Waren scannt. Damit stellte sich die Frage nach der Möglichkeit und Zulässigkeit einer sekundengenauen Arbeitnehmerüberwachung.
Die Mitarbeiter müssen die Handscanner an einer Ausgabestation nach Registrierung abholen und dabei auch ihren Mitarbeiterausweis einscannen. Die Speicherung der Personalnummer ist nach Angaben der Ansprechpartner erforderlich, weil damit erst der Zugang zur Datenbank eröffnet wird und somit die Rechtezuordnung gewährleistet ist. Nach Erledigung der Aufträge wird der Handscanner zurückgegeben. Der Mitarbeiter loggt sich aus. Der Zeitpunkt der Rückgabe wird deshalb erfasst, weil in der Vergangenheit immer wieder derartige Handscannergeräte abhandengekommen waren. Die erfassten Daten werden in einer der Lagerverwaltung dienenden Datei gespeichert. Aus diesen Daten können so genannte Revisionslisten erzeugt werden, die im Falle von vermehrten Retoursendungen eine Überprüfung ermöglichen und damit zur Fehlervermeidung beitragen, weil gegebenenfalls Abläufe optimiert werden können. In einer Teilkonzernrahmenbetriebsvereinbarung, die in der Betriebsstätte umzusetzen ist, ist niedergelegt, dass eine Leistungs- und Verhaltenskontrolle grundsätzlich nicht zulässig ist. Die datenschutzrechtliche Prüfung und Bewertung aller in diesem Zusammenhang nachträglich durch die verantwortliche Stelle übermittelten Dokumente ist noch nicht abgeschlossen.

Werden in einem Unternehmen Handscanner eingesetzt, mittels deren Speicherung der einzelnen Handlungen ein sekundengenaues Tätigkeitsprofil des Mitarbeiters erstellt werden kann, ist sicherzustellen, dass eine solche Leistungs- und Verhaltenskontrolle ausgeschlossen ist.

5.20 Fahrzeugvermittlung nur gegen Mitarbeiterdaten?

Ein Fuhrparkunternehmen bietet einen Autoabhol- und -bringservice an. Das Unternehmen holt Ihr Fahrzeug beispielsweise für Sie am

Geschäftsort ab und bringt es Ihnen nach Hause. Einige Kunden des Fuhrparkunternehmens verlangten vor der Übergabe ihrer Fahrzeuge an das Unternehmen die Kopie des Personalausweises der Mitarbeiter. Diese hatten berechtigte Bedenken dabei. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) konnte in diesem Fall nur beratend tätig werden, da die verantwortliche Stelle (Kunden des Unternehmens) vom Beschwerdeführer nicht benannt wurde und somit unbekannt blieb.
Nach § 14 Nr. 2 des Personalausweisgesetzes (PAuswG) darf die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises durch nicht-öffentliche Stellen nur nach §§ 18 bis 20 PAuswG erfolgen. Danach ist das Anfertigen von Kopien datenschutzrechtlich nicht zulässig, es sei denn, sie ist durch eine spezielle gesetzliche Ermächtigung erlaubt. Dies war im vorliegenden Sachverhalt nicht der Fall. Zum Nachweis der Identität ist es ausreichend, sich den Personalausweis vorlegen zu lassen und hierüber ggf. einen Vermerk zu machen, der allein die notwendigen Identitätsdaten wie Vorname, Name und Anschrift enthält. Personalausweise und Reisepässe sind ohnehin nicht als „Pfand“ geeignet. Beide Dokumentarten sind Eigentum der Bundesrepublik Deutschland (§ 2 Abs. 2 PAuswG, § 4 Abs. 4 PassG).

Das Erstellen von Personalausweiskopien zum Nachweis der Identität einer Person ist nicht erforderlich, wenn der Personalausweis eingesehen werden kann. Kopien des Personalausweises sowie des Reisepasses sind damit unzulässig.

5.21 Handydaten auf Achse

Nicht selten wenden sich betriebliche Datenschutzbeauftragte (bDSB) direkt an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), wenn in einem Unternehmen datenschutzrechtliche Missstände zu verzeichnen sind. So war es auch in einem besonders schweren Fall einer Mitarbeiterüberwachung. Ein betrieblicher Datenschutzbeauftragter meldete dem TLfDI gleich zwei Fälle: Überwachung von E-Mail-Konten und Überwachung von Telefondaten der Angestellten eines Verbands. Dabei hatte der Verbandsvorsitzende zu Vertretungszwecken Zugriff auf drei Mitarbeiter-E-Mail-Konten. Diese Zugriffsrechte nutzte der Verbandsvorsitzende aus, um die E-Mails eines Mitarbeiters zu kon-

trollieren. Besonders problematisch dabei war, dass die Nutzung des E-Mail-Postfaches auch für private Zwecke geduldet wurde. Die rechtlichen Grundlagen bei der Nutzung von E-Mail finden sich im Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG), den dienstrechtlichen Vorschriften sowie den allgemeinen Vorschriften des Bundesdatenschutzgesetzes. Lässt der Arbeitgeber private E-Mails zu, wird er selbst zum Telekommunikationsanbieter, der das Telekommunikationsgeheimnis bei den privaten E-Mails zu wahren hat, diese also nicht zur Kenntnis nehmen darf. Der Arbeitgeber hatte in diesem Fall das Fernmeldegeheimnis nach § 88 des TKG zu beachten. Jeder Zugriff auf das E-Mail-Konto eines Mitarbeiters stellt eine Straftat nach § 88 Abs. 3 TKG dar. Es gibt allerdings gerichtliche Entscheidungen, nach denen der Arbeitgeber in Notsituationen auf das E-Mail-Konto des Arbeitgebers zugreifen darf. In diesen Fällen muss jedoch der Arbeitgeber zwischen den eigenen Interessen und dem Persönlichkeitsrecht der informationellen Selbstbestimmung des betroffenen Mitarbeiters abwägen. Die Einführung und nähere Ausgestaltung der E-Mail-Nutzung durch die Beschäftigten in einem Betrieb unterliegt der Mitbestimmung des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG.

Weiterhin hatte der Verbandsvorsitzende zwei Dienstleistungsverträge für die Diensttelefone der Angestellten bei einem Telekommunikationsunternehmen abgeschlossen. In den Verträgen wählte er nach eigenem Ermessen hinsichtlich der Verbindungsnachweise die Option der vollständigen Anzeige der Zielrufnummern. Die dafür erforderliche Zustimmung des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG lag nicht vor. Dadurch wurden personenbezogene Daten Dritter, nämlich der angerufenen Personen, erhoben und gespeichert. Speichern stellt nach § 3 Abs. 4 BDSG eine Datenverarbeitung dar. Erheben ist nach § 3 Abs. 3 BDSG das Beschaffen von Daten über den Betroffenen. Nach § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten beim Betroffenen zu erheben. Davon ist nur in den abschließend aufgeführten Fällen des § 4 Abs. 2 Satz 1 BDSG eine Ausnahme zu machen. Eine solche war hier jedoch nicht einschlägig. Diese Ausnahmen greifen nur dann, wenn hierfür eine Rechtsvorschrift existiert, die dies ausdrücklich erlaubt oder erzwingt, der Geschäftszweck des Vereins dies erforderlich macht oder die Direkterhebung mit einem unverhältnismäßigen Aufwand verbunden ist. Eine Einwilligung der Betroffenen kam der Natur der Sache nach nicht in Betracht. Als Erlaubnisnorm schied § 28 BDSG aus. Für den

Bereich des Arbeitnehmerdatenschutzes hat der Gesetzgeber mit § 32 BDSG eine abschließende Norm geschaffen, die im Verhältnis zu § 28 BDSG spezieller ist und dessen Anwendung in diesem Zusammenhang daher ausschließt. Ob eine Datenerhebung nach § 32 Abs. 1 Satz 1 BDSG vorliegend erforderlich war, kann dahinstehen. Die private Nutzung der Diensttelefone hatte der Verein geduldet. Auch hier unterfällt der Arbeitgeber dem Fernmeldegeheimnis nach § 88 Abs. 1 TKG. Zur Erfüllung des Geschäftszweckes des Vereins war es nicht erforderlich, die Telefondaten Dritter zu erheben und zu speichern. Der Verein hatte Telefondaten unzulässig erhoben und gespeichert.
Auf Eigeninitiative der zuständigen Angestellten wurde ein Antrag auf einen Einzelverbindungsnachweis mit verkürzten Rufnummern gestellt. Der Telekommunikationsanbieter stellte den Einzelverbindungsnachweis sofort auf die verkürzte Rufnummernanzeige um und bestätigte dies gegenüber dem Verband. Die unzulässige Datenerhebung und -speicherung von Telefondaten Dritter wurde damit beendet. Der Verbandsvorsitzende schied unmittelbar nach dem Bekanntwerden der oben dargestellten Vorfälle aus dem Verein aus. Dies hinderte den TLfDI allerdings nicht daran, ein Bußgeldverfahren gegen den ehemaligen Verbandsvorsitzenden durchzuführen.

Die rechtlichen Grundlagen bei der Nutzung von Telekommunikationsdiensten (E-Mail, Telefon) finden sich im TKG, dem TMG, den dienstrechtlichen Vorschriften sowie den allgemeinen Vorschriften des Bundesdatenschutzgesetzes. Lässt der Arbeitgeber private E-Mails und Telefonate zu bzw. duldet er diese, wird er selbst zum Telekommunikationsanbieter, der das Telekommunikationsgeheimnis zu wahren hat und damit die erhobenen Daten nicht zur Kenntnis nehmen darf. Der Arbeitgeber hatte in diesem Fall das Fernmeldegeheimnis nach § 88 des TKG zu beachten. Jeder Zugriff auf das E-Mail-Konto eines Mitarbeiters und die Erhebung der Telefondaten stellt eine Straftat nach § 88 Abs. 3 TKG dar. Es gibt allerdings gerichtliche Entscheidungen, nach denen der Arbeitgeber in Notsituationen auf das E-Mail-Konto des Arbeitgebers zugreifen darf.

5.22 Mitarbeiterüberwachung durch technische Vorrichtungen

Aus der Presse hatte ein Hinweisgeber entnommen, dass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfrei-

heit (TLfDI) bei der in Thüringen ansässigen Niederlassung eines großen überregionalen Unternehmens eine datenschutzrechtliche Prüfung wegen Mitarbeiterüberwachung durch Handscanner durchführte. Zu den in der Presse geschilderten Aktivitäten zur Mitarbeiterüberwachung sah er Parallelen auch in dem Unternehmen, in dem er als Zeitarbeiter beschäftigt gewesen war und legte dar, selbst Pausen, Toilettengänge und die Länge der Ausführung von Aufträgen, so genannten Calls, würden protokolliert und den Mitarbeitern vorgehalten.

Es gehört nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) zu den Aufgaben des TLfDI, die Ausführung datenschutzrechtlicher Bestimmungen bei allen nicht-öffentlichen Stellen in Thüringen zu kontrollieren. Die sachliche Zuständigkeit hierzu ergibt sich aus § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 BDSG, die örtliche Zuständigkeit für Thüringen ergibt sich für selbstständige Niederlassungen aus § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG.)

Im Rahmen der Bearbeitung einer Beschwerde ist zur Feststellung der sachlichen und örtlichen Zuständigkeit für eine Niederlassung zunächst zu prüfen, ob das Unternehmen in Thüringen (eigen) verantwortliche Stelle in Sinne des § 3 Abs. 7 BDSG ist. Anhand von Internetauftritten und des Handelsregisterauszugs sind die Verflechtungen im Konzern und Kompetenzen von Niederlassungen oftmals nicht oder nur sehr schwer erkennbar. Auch Nachfragen bei anderen Landesdatenschutzbeauftragten ergeben bisweilen nicht den nötigen Aufschluss.

Bei dem betroffenen Unternehmen war der Zusammenhang mit einem großen, weltweit vertretenen Konzern zu erkennen. Zur Klärung des Sachverhalts kündigte daher der TLfDI eine datenschutzrechtliche Kontrolle nach § 38 Abs. 4 BDSG an und bat um Bereithaltung von Unterlagen. Daraufhin meldete sich die Datenschutzabteilung des Konzerns, die in einem anderen Bundesland angesiedelt ist und teilte mit, der bestellte Konzerndatenschutzbeauftragte sei auch für die Niederlassung in Thüringen zuständig. Man wolle selbstverständlich kooperativ sein, habe jedoch Interesse daran, vorab die Zuständigkeit des TLfDI eindeutig festzustellen, zumal die Niederlassung Thüringen zu einer Gesellschaft gehöre, die in einem dritten Bundesland gemeldet sei.

Aufgrund der ausstehenden notwendigen Informationen wurde die Kontrolle daher zurückgestellt, um zu prüfen, auf welche konkreten

Datenverarbeitungen sie sich zuständigkeitshalber beziehen kann. Für Bereiche, die durch Konzernvereinbarungen oder in Gesamtbetriebsvereinbarungen geregelt sind und für die keine eigene Entscheidungskompetenz der Betriebsstätte für die Datenverarbeitung in Thüringen existiert, besteht keine ausschließliche Kontrollkompetenz des TLfDI. Die Kontrolle muss in solchen Fällen immer mit der am Hauptsitz des Konzerns zuständigen Aufsichtsbehörde abgestimmt werden.
Insoweit unterlägen der datenschutzrechtlichen Kontrolle des TLfDI in besagter Niederlassung nur wenige Bereiche. Über das Ergebnis wird im nächsten Tätigkeitsbericht informiert.

Handelt es sich bei einer Betriebstätte in Thüringen um eine Niederlassung eines überregionalen Unternehmens, ist zu prüfen, ob die Niederlassung eine eigene Entscheidungskompetenz hinsichtlich der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten hat. Die Zuständigkeit zur Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben für den TLfDI ist dann gegeben, wenn der Niederlassung eine Entscheidungskompetenz zukommt. Konzernvereinbarungen und Gesamtbetriebsvereinbarungen, die dem Hauptunternehmen zuzuordnen sind, das sich in einem anderen Bundesland befindet, unterliegen nicht der Prüfung durch den TLfDI. Gegebenenfalls wird der Datenschutzbeauftragte des Bundeslandes, in dem das Hauptunternehmen seinen Sitz hat, eingeschaltet.

5.23 Kündigung – Zugriff des Arbeitgebers auf private Daten des Arbeitnehmers auf dem Arbeitsplatzrechner?

Eine private Fachhochschule bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung, wie mit einem Arbeitsplatz-PC bei Beendigung des Arbeitsverhältnisses umzugehen ist. In dem speziellen Fall sollten mit Ausscheiden eines Mitarbeiters dessen Zugriffsmöglichkeiten auf den PC unmittelbar entzogen werden. Der TLfDI stellte zunächst fest, dass dieses zulässig ist, da der PC grundsätzlich im Eigentum der Fachhochschule steht. Die Fachhochschule hat darüber hinaus nach § 9 Bundesdatenschutzgesetz (BDSG) sogar die Pflicht, Maßnahmen zu ergreifen, um eine Kenntnis von personenbezogenen Daten durch Unbefugte zu verhindern. Der weitere Zugang eines ausgeschiedenen Mitarbeiters auf dienstliche Unterlagen der Hochschule ist deshalb

zu verhindern. Sind aber noch private Dateien des Mitarbeiters gespeichert, etwa private E-Mails oder Daten im Home-Verzeichnis der Festplatte des Rechners, darf die Hochschule diese privaten Dateien nicht ohne Weiteres öffnen oder löschen, sondern muss die Rechte des ausscheidenden Mitarbeiters beachten. Wenn die Hochschule ihren Beschäftigten die private Nutzung von E-Mail und Internet erlaubt, erbringt sie ihren Mitarbeitern gegenüber geschäftsmäßig Telekommunikationsdienste. Die Fachhochschule hat dann das Fernmeldegeheimnis zu wahren. Daher sind Zugriffe und Löschungen der privaten E-Mails durch den Arbeitgeber nur mit ausdrücklich erteilter Einwilligung des Betroffenen gemäß § 4a Bundesdatenschutzgesetz zulässig. Auch wenn die Fachhochschule die private Nutzung des E-Mail-Verkehrs nicht ausdrücklich erlaubt oder verboten hat und die private Nutzung regelmäßig duldet, kommt ebenfalls das Telekommunikationsgesetz mit den o. g. Folgen zur Anwendung. War die E-Mail-Nutzung hingegen ausdrücklich nur zu betrieblichen Zwecken erlaubt, darf die Hochschule als Arbeitgeber allerdings in das E-Mail-Postfach des ausscheidenden Mitarbeiters Einsicht nehmen, da davon ausgegangen werden kann, dass nur dem Arbeitgeber zustehendes Schriftgut vorhanden ist. Sobald jedoch festgestellt wird, dass E-Mails privaten Charakter aufweisen, dürfen diese vom Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden. Hatte der Mitarbeiter bestimmte private Verzeichnisse auf der Festplatte des Rechners oder innerhalb des E-Mail-Accounts angelegt und sind diese klar gekennzeichnet, so hat dieser zwar gegen die betrieblichen Anweisungen der Hochschule verstoßen, aber auch hier darf aus datenschutzrechtlicher Sicht der Arbeitgeber in die Dateien keine Einsicht nehmen und die Dateien auch nicht einfach löschen. Vielmehr ist dem ausscheidenden Mitarbeiter die Gelegenheit zu geben, eingegangene E-Mails auf dem ihm zugewiesenen Account auf private Inhalte durchzusehen und diese zu löschen. Dies gilt ebenso für weitere private Dateien, die auf dem Rechner gespeichert sind. Um Konflikte zwischen Arbeitgeber und Arbeitnehmer von vornherein auszuschließen, sollte der Arbeitgeber die genaue Verfahrensweise beim Umgang mit privaten Dateien in einer Betriebsvereinbarung ausdrücklich regeln. Mit dieser Auskunft war die Hochschule zufrieden, sie hat sich nicht mehr gemeldet.

Wertvolle Hinweise zur Regelung und zum Abschluss einer entsprechenden Betriebsvereinbarung enthält die „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung

von E-Mail und anderen Internetdiensten am Arbeitsplatz“, die jedoch erst nach Schluss des Berichtzeitraums beschlossen wurde und seit Februar 2016 auf der Internetseite des TLfDI verfügbar ist.

Dem Arbeitgeber ist es nicht erlaubt, beim Ausscheiden von Mitarbeitern ohne Einwilligung der Betroffenen in private E-Mails Einblick zu nehmen oder diese zu löschen. Es wird empfohlen, den Umgang mit privaten E-Mails der Beschäftigten bei deren Ausscheiden in einer Betriebsvereinbarung zu regeln.

Kreditkarte Schloss Online – © Calado / Fotolia.com

6 Kreditinstitute

6.1 Bankgeheimnis?

Ein Beschwerdeführer sah durch eine Bank das Bankgeheimnis verletzt. Mit dieser Bank befand sich der Beschwerdeführer vor einigen Jahren im Rechtsstreit. Damals hatte die Bank einen Vollstreckungsbescheid erwirkt, den sie bislang nicht vollstrecken konnte. Also passierte einige Zeit nichts. Plötzlich wurden jedoch das Konto der Ehefrau des Beschwerdeführers bei einer anderen Bank sowie ihr Lohnanspruch gegen ihren Arbeitgeber aufgrund eines erwirkten Pfändungs- und Überweisungsbeschlusses gepfändet.
Weshalb nun plötzlich die Gläubigerbank pfänden konnte, lag nach Auffassung des Beschwerdeführers daran, dass der Arbeitgeber der Ehefrau ausgerechnet zu seiner Gläubigerbank gewechselt hatte. Diese überwies nun die Löhne – auch an die Ehefrau des Beschwerdeführers. Damit hatte die Bank natürlich auch Kenntnis über den Arbeitgeber und das Lohnkonto der Ehefrau.
Datenschutzrechtlich sind Kundendaten und die damit zusammenhängenden Kontobewegungen personenbezogene Datenverarbeitungen für die Erfüllung eigener Geschäftszwecke (§ 28 Bundesdaten-

schutzgesetz). Diese Daten dürfen für die Abwicklung der Aufträge verarbeitet und genutzt werden. Eigene Geschäftszwecke liegen unter anderem auch vor, wenn vollstreckbare Forderungen vorliegen. Weiterhin muss das Vorliegen eines schutzwürdigen Interesses der davon Betroffenen an dem Ausschluss der Übermittlung oder Nutzung geprüft werden. Liegt eine vollstreckbare Forderung vor, kann jeder Gläubiger, sobald er Kenntnis davon erhält, dass Vermögen oder Drittschuldner vorhanden sind, eine Vollstreckung betreiben. Ein schutzwürdiges Interesse der von der Vollstreckung Betroffenen dahingehend, dass diese bekannt gewordenen personenbezogenen Vermögensdaten bzw. die bekannt gewordenen Ansprüche an Drittschuldner einer Vollstreckung entzogen werden könnten, liegt grundsätzlich nicht vor. Ein Verstoß gegen datenschutzrechtliche Vorschriften war daher nicht offensichtlich erkennbar.
Selbstverständlich liegt in einem solchen Zusammenhang die Bevorzugung von Banken vor, da eine Privatperson entsprechende Kenntnis kaum oder nur schwer erhalten kann. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat dem Beschwerdeführer angeboten, als Datenschutzaufsichtsbehörde die konkrete Datenverarbeitung bei der Bank zu überprüfen. Von diesem Angebot hat er allerdings keinen Gebrauch gemacht. Möglicherweise hätte diese Überprüfung auch nicht den gewünschten Erfolg versprochen, denn selbst wenn Umstände vorlägen, die eine Nutzung der Erkenntnisse der Bank für Zwecke der Forderungseintreibung unzulässig machten, verhindert dies die in Gang gesetzte Vollstreckung nicht. Eine mögliche datenschutzrechtliche Unzulässigkeit der Nutzungs- und Kontodaten kann eine Pfändung nicht verhindern.

Liegt ein Pfändungs- und Überweisungsbeschluss vor, kann ein Gläubiger in Konten des Schuldners oder in dessen Vermögen, das ihm bekannt geworden ist, vollstrecken. Selbst wenn die Daten unzulässig erlangt worden wären, verhindert dies eine Pfändung nicht.

6.2 Bei Anruf kein Bankgeheimnis?

Ein Beschwerdeführer hatte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt, weil die Kontoauszüge zu seinen Konten an eine andere Wohnadresse gesandt worden waren. Damit konnte eine andere Person seine Kontenbewegungen zur Kenntnis nehmen.

Bei der Sachverhaltsaufklärung stellte sich heraus, dass es sich bei der anderen Wohnadresse um die Adresse seiner geschiedenen Ehefrau handelte. Die Adressänderung zu den Konten des Beschwerdeführers war von der Bank aufgrund einer telefonischen Kundenmitteilung nach Abfrage seiner Identifikationsdaten vorgenommen worden. Wer diese Adressänderung veranlasst hatte, ließ sich nicht mehr ermitteln. Der Beschwerdeführer war es jedenfalls nicht. Zur Legitimation bei einem telefonischen Auftrag werden die Kontonummer, der Name, das Geburtsdatum, der Geburtsort sowie die bisherige Anschrift des Kontoinhabers abgefragt. Die Angaben wurden in diesem Fall auch schriftlich festgehalten. Dieser Adressänderungsprozess erfolgte auf Basis des gängigen Standards und war in der Organisationsrichtlinie der Bank festgelegt. Weitergehende Überprüfungen, so wurde auf Nachfrage mitgeteilt, seien nicht vorgesehen gewesen.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Im Zusammenhang mit einem Kontenvertrag ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich ist (§ 28 Abs. 1 Nr. 1 BDSG). Das Schuldverhältnis ist vertraglich geregelt. Nach den allgemeinen Geschäftsbedingungen hat der Kunde die Veränderungen seiner Anschrift unverzüglich der Bank mitzuteilen. Hierzu befugt sind nach dem hierfür vorgesehenen Formular zur Erteilung einer Kontovollmacht der Kontoinhaber selbst sowie ggf. ein gesetzlicher Vertreter und Bevollmächtigte als vertragliche Vertreter. Die vertraglich festgelegten Sicherheiten zur Legitimation bieten, wie der vorliegende Fall zeigt, zwar keinen Schutz gegen Missbrauch durch andere Personen, deren Legitimation zwischenzeitlich entfallen ist, wenn die Daten durch die tatsächlich befugten Kontoinhaber nicht geändert werden. Mit dem Abschluss des Kontovertrags haben Bankkunden sich mit dem Verfahren schriftlich einverstanden erklärt.

Aufgrund der Beschwerde hat die Bank jedoch unverzüglich den weiteren Telefonverkehr zu diesen Konten ausgeschlossen. Somit kann zumindest für die Zukunft sichergestellt werden, dass Aufträge nur noch schriftlich eingereicht werden können.

Ist vertraglich vereinbart, dass Änderungen zu einem Bankkonto telefonisch mitgeteilt werden können, ist darauf zu achten, dass die Identifikationsdaten anderen Personen nicht zur Kenntnis gelangen. Sollten sie dennoch auch anderen Personen bekannt sein, empfiehlt sich eine umgehende Änderung durch den Kontoinhaber.

6.3 E-Mail-Verschlüsselung auch bei der Bank?

Ein Bankkunde hat sich mit einer Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Er beschwerte sich darüber, dass auf seine Online-Anfrage bei einer Bank eine Mitarbeiterin per E-Mail geantwortet habe. Im Anhang befand sich ein Antwortschreiben mit seiner Bankverbindung und vollständiger Kreditkartennummer. Diese E-Mail war nicht verschlüsselt.
Gemäß § 9 Bundesdatenschutzgesetz (BDSG) haben nicht-öffentliche Stellen, wie hier die Bank, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage des BDSG genannten Anforderungen, zu gewährleisten. Danach hat die Bank also sicherzustellen, dass die personenbezogenen Daten der Bankkunden bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Personenbezogene Daten sind dabei solche Angaben, welche über die persönlichen oder sachlichen Verhältnisse des Betroffenen Auskunft geben, vergleiche § 3 Abs. 1 BDSG. Nach § 9 BDSG geht es insbesondere darum, je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignete Maßnahmen zu treffen. Nachdem der TLfDI die Bank zur Stellungnahme zu den nach § 9 BDSG getroffenen technischen oder organisatorischen Maßnahmen aufforderte, antwortete die Bank wie folgt:
Bei der Beantwortung der Online-Anfrage des Bankkunden habe die bearbeitende Mitarbeiterin aufgrund der Dringlichkeit nicht die normalerweise übliche Sorgfalt walten lassen und habe deshalb die Angaben in einem unverschlüsselten Anhang per E-Mail an den Bankkunden versandt. Üblicherweise würde die Bank in derart gelagerten Fällen so verfahren, dass sie solche Dokumente über das On-

line-Banking-Portal den Kunden zukommen lässt. Es habe sich vorliegend um einen bedauerlichen Ausnahmefall gehandelt, den die Bank zum Anlass genommen habe, erneut die Mitarbeiter zu diesem Thema zu sensibilisieren.
Weiterhin teilte die Bank dem TLfDI die von ihr ergriffenen technischen und organisatorischen Maßnahmen zur gesicherten Datenübertragung mit. Über das abgesicherte Online-Banking-Portal würde die Möglichkeit bestehen, mit Bankkunden gesichert und verschlüsselt Informationen auszutauschen. Dieses soll grundsätzlich von den Mitarbeitern immer genutzt werden, wenn Kunden auch Online-Banking-Nutzer sind. Im Rahmen einer Arbeitsanweisung habe die Bank ihre Mitarbeiter dazu verpflichtet, keine E-Mails ungesichert über das Internet zu versenden, die sensible Kundendaten (Kontostände, Kontodaten, persönliche Daten usw.) enthalten. Weiterhin seien die Mitarbeiter angewiesen, entsprechende Anfragen von Bankkunden mit dem Verweis auf sicherheits- und datenschutzrechtliche Regelungen abzulehnen und, sofern ein Versand von personenbezogenen Daten per E-Mail unabdingbar sei, dass diese E-Mails grundsätzlich mit 7-Zip passwortgeschützt zu verschlüsseln sind. Dafür installierte die Bank auf jeden Bankrechner das Programm 7-Zip. Auch sei in der Arbeitsanweisung eine Anleitung, wie das Programm und welche Verschlüsselungsstärke angewendet werden müsste, enthalten. Schließlich seien die Mitarbeiter noch angehalten, das verwendete Passwort über einen anderen Kommunikationskanal an den Empfänger zu übermitteln.
Mit dieser Mitteilung konnte der TLfDI das Verwaltungsverfahren abschließen.

Die von nicht-öffentlichen Stellen zu treffenden technischen und organisatorischen Maßnahmen dienen dem Schutz der Persönlichkeitsrechte und damit der technisch-organisatorischen Umsetzung des BDSG. Nach § 9 BDSG haben nicht-öffentliche Stellen (also vor allem privatwirtschaftliche Unternehmen), soweit sie personenbezogene Daten erheben, verarbeiten oder nutzen, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um allgemein die Anforderungen des BDSG zu erfüllen, vor allem aber die in der Anlage zu § 9 BDSG genannten „Gebote“. Einschränkend gilt, dass nur die technisch-organisatorischen Maßnahmen erforderlich sind, bei denen der dafür nötige Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht, § 9 Satz 2 BDSG.

6.4 Datenschutz: Bloß nicht die Kontonummer und Bankleitzahl verraten?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Bürgers, dass ein in Thüringen ansässiger Paid-Mailer trotz Einführung des neuen IBAN-Verfahrens und dem Verlangen der Internationalen Kontonummer „ISO“ (IBAN) und „Bank Identifier Code“ zur weltweit eindeutigen Identifizierung von Kreditinstituten (BIC) weiterhin auf die Angabe von Bankleitzahl und Kontonummern der Empfänger bestanden hatte. Paid-Mailer oder Paid-Dienste sind Werbeanbieter aus dem Internet, welche die Empfänger für das Lesen von Werbe-E-Mails (Paidmails) bezahlen. Die Paidmail-Anbieter verschicken hierbei Onlinewerbung für Firmen wie Onlineshops oder kommerzielle Webseiten in Form so genannter Paidmails (bezahlte Emails). Die werbenden Unternehmen schätzen diese Form des E-Mail-Marketings, da Werbung über Paidmail-Anbieter die günstigste Form echter Unique Visitors Unique Visit (engl.: ist eine Metrik der Zugriffshäufigkeit einer Webseite) ist. Werben die Paidmail-Anbieter für das werbende Unternehmen selbst einen User, erhalten diese von den werbenden Unternehmen einen höheren Verdienst. Im Gegensatz zu Spammails erhält der Empfänger die Paidmails nur auf ausdrücklichen Wunsch, in Form einer Registrierung beim Paidmailer. Damit erklärt der Empfänger sich bereit, E-Mails mit werbendem Inhalt zu empfangen, diese zu öffnen und zu lesen.
In einem Auskunftsverlangen wandte sich daraufhin der TLfDI an den Paid-Mailer mit der Bitte um Auskunft, auf welcher rechtlichen Grundlage die Nachfrage bei den Empfängern beruhte, sowohl die Angabe der IBAN und BIC als auch die Angabe von Bankleitzahl und Kontonummer zu verlangen. Denn nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als Erlaubnisnorm kam vorliegend der § 28 Abs. 1 Nr. 1 BDSG in Betracht. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendi-

gung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1).
Im Ergebnis erläuterte der Paid-Mailer dem TLfDI ausführlich den Hintergrund, warum er zum damaligen Zeitpunkt beide Angaben zu den Kontodaten hinterfragt hatte. Denn ab 1. Februar 2016 wird der einheitliche europäische Zahlungsverkehr SEPA den bisherigen nationalen Zahlungsverkehr endgültig ablösen.
Vor allem wollte er den Empfängern eine Auszahlung auf dem herkömmlichen Weg ermöglichen. Denn oft konnten die Nutzer seiner Seite mit den Begriffen IBAN und BIC nichts anfangen.
Gegen diese Praxis war aus datenschutzrechtlicher Sicht des TLfDI nichts einzuwenden, denn das Erheben der Kontonummer und der Bankleitzahl war im Sinne des § 28 Abs. 1 Nr. 1 BDSG für die Durchführung des Rechtsgeschäfts zu den Werbe-Email-Empfängern erforderlich. Das Verfahren konnte abgeschlossen werden.

Das Abfragen von Kontonummer und Bankleitzahl (bis zum 1. Februar 2016 durch endgültiges Ablösen durch den einheitlichen europäischen Zahlungsverkehr SEPA) als auch von IBAN und BIC ist als Mittel für die Erfüllung eigener Geschäftszwecke dann zulässig, wenn diese Daten zur Durchführung des rechtsgeschäftlichen Schuldverhältnisses erforderlich sind, § 28 Abs. 1 Nr. 1 BDSG. Dies ist insbesondere dann der Fall, wenn die verantwortliche Stelle dem Betroffenen Geld überweisen möchte, wie in diesem Fall.

Lupe Schufa – © JiSign / Fotolia.com

7 Auskunfteien

7.1 Eigentümerdaten aus 2. Hand

In einem Beratungsgespräch trugen Eigentümer eines Grundstücks dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vor, ein Kaufangebot eines Immobilienunternehmens für ihr Anwesen erhalten zu haben. Die Eigentümer wunderten sich, warum auch die verstorbene Schwester im Anschreiben des Unternehmens angesprochen wurde. Da der Name der verstorbenen Schwester nicht am Klingelschild des Hauses zu finden war, konnten sich die Eigentümer diesen Umstand nur mit einer Abfrage im Grundbuch erklären, in dem die Verstorbene noch als Miteigentümerin eingetragen war. Sie erkundigten sich beim TLfDI nach der Zulässigkeit dieser Vorgehensweise und baten, diesen Sachverhalt zu überprüfen.
Natürlich ging der TLfDI diesem kuriosen Fall auf den Grund. Zunächst befragte der TLfDI das zuständige Grundbuchamt zu der Angelegenheit. Dort lag kein Antrag auf einen Grundbuchauszug oder Gesuch auf Einsicht in das Grundbuch vor. Das Grundbuchamt wies deutlich darauf hin, dass ein Kaufinteressent die Vollmacht des

Eigentümers vorlegen muss, es sei denn, es ist ein Recht für den Kaufinteressenten eingetragen (Abteilung II oder III). Auf Nachfrage des TLfDI beim Immobilienunternehmen teilte dieses mit, dass es eine entgeltliche Auskunft vom Thüringer Landesamt für Geoinformation und Vermessung (TLVermGeo) eingeholt habe. Bei einer Fahrt durch Erfurt sei den Mitarbeitern des Immobilienunternehmens das gegenständliche Gebäude aufgefallen und man habe die Eigentümer recherchiert. Berechtigtes Interesse für den Antrag an das TLVermGeo sei gewesen, Kontakt mit den Käufern aufzunehmen, um ein Kaufangebot zu unterbreiten bzw. alternativ eine Innenbesichtigung vorzunehmen. Damit wollte das Immobilienunternehmen feststellen, ob diese Immobilie seinen gewünschten Anforderungen entspreche. Es suchte eine Immobile für seine Kunden und auch zum Eigennutz. Der TLfDI brachte weiterhin in Erfahrung, dass eine weitere Speicherung personenbezogener Daten im System des Immobilienunternehmens nicht erfolgt war, da sich die Eigentümer der besagten Immobilie nicht gemeldet hatten. Deren Daten wurden auch nicht an Dritte weitergegeben und ferner nicht Dritten zur Einsicht oder zum Abruf bereitgestellt.
Das TLVermGeo erteilt Auskünfte aus dem Liegenschaftskataster, in dem die Eigentümerdaten in Übereinstimmung mit dem Grundbuch nachrichtlich geführt werden. Die Auskunft zu den Eigentümerdaten bezüglich der streitgegenständlichen Immobilie sei nach Auskunft des TLVermGeo auf Grundlage von Bestimmungen des Thüringer Vermessungs- und Geoinformationsgesetzes (ThürVermGeoG) erfolgt. So bestehe gemäß § 2 ThürVermGeoG eine der wesentlichen Aufgaben des amtlichen Vermessungswesens in der Führung des Liegenschaftskatasters einschließlich der Aufbereitung der Daten zu Geoinformationen und deren Bereitstellung zur Nutzung. Die Bereitstellung personenbezogener Daten erfahre dabei gemäß § 18 Abs. 1 ThürVermGeoG die Einschränkung, dass beantragende Personen oder Stellen ein berechtigtes Interesse an der Kenntnis der Daten haben müssten. Zum berechtigten Interesse zähle auch ein wirtschaftliches Interesse, welches sich aus dem Auftrag des Amtlichen Vermessungswesens ableite. Danach sei das Liegenschaftskataster auch den Anforderungen der Wirtschaft bereitzustellen. Im Ergebnis wurde in Abwägung der Interessen des Immobilienunternehmens einerseits und der Eigentümerinteressen andererseits das Vorliegen eines wirtschaftlichen Interesses vom TLVermGeo anerkannt. Die bestehende Diskrepanz zwischen der begrüßenswert generell zu-

rückhaltenden Auskunftserteilung durch das Grundbuchamt und der freigiebigen Auskunftserteilung des Liegenschaftskatasters ist dem TLfDI hierbei aufgefallen. Dies wird der TLfDI einer Prüfung unterziehen.
In der Sache selber konnte kein datenschutzrechtlicher Verstoß auf Seiten des Immobilienunternehmens festgestellt werden. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) zwar nur zulässig, wenn eine Rechtsvorschrift innerhalb oder außerhalb des BDSG dies erlaubt oder der Betroffene eingewilligt hat. Allerdings war die Datenerhebung für die Erfüllung der Geschäftszwecke des Immobilienunternehmens zulässig, da die personenbezogenen Eigentümerdaten für die Begründung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich waren und das Kaufinteresse im Namen des Immobilienunternehmens bekundet worden und daher nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt war. Eine Übermittlung oder Nutzung der erhobenen personenbezogenen Daten für einen anderen Zweck wäre unzulässig gewesen.
Der TLfDI wies das Immobilienunternehmen deutlich darauf hin, dass jedenfalls auch eine Nutzung der geschäftlich erhobenen Daten für private Zwecke unzulässig ist.

Eine Auskunft aus dem Liegenschaftskataster begegnet nicht den gleichen Hürden wie ein Auszug aus dem Grundbuch. Eine Auskunft aus dem Liegenschaftskataster ist aber auch nicht ohne Weiteres für jedermann möglich. Das antragstellende Unternehmen muss ein berechtigtes Interesse daran darlegen. Vor der Auskunft muss das Thüringer Landesamt für Vermessung und Geoinformation sorgfältig abwägen, ob das dargelegte berechtigte Interesse die schutzwürdigen Interessen der Betroffenen überwiegt.

7.2 Auskunfteien: datenschutzrechtlicher Quell der "Freude"

Große Auskunfteien wie die Schufa oder Bürgel befinden sich nicht in Thüringen. Bei Anfragen und Beschwerden zu dort gespeicherten Daten verweist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an die hierfür zuständigen Aufsichtsbehörden.
Für die in Thüringen ansässigen Auskunfteien aber auch für Unternehmen oder Banken aus Thüringen, die Daten an Auskunfteien

übermitteln oder Daten dort abfragen, ist der TLfDI zuständige Aufsichtsbehörde. Haben Unternehmen die geschuldete Leistung erbracht und wurde vom Schuldner die Forderung trotz Fälligkeit nicht erfüllt, soll eine Auskunftei oftmals Angaben über die Zahlungsfähigkeit des Schuldners machen. Dies ist zulässig, soweit die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und die in § 28a Abs. 1 Bundesdatenschutzgesetz (BDSG) genannten Voraussetzungen vorliegen. Auch Kreditinstitute dürfen personenbezogene Daten mit der Begründung, dies sei zur ordnungsgemäßen Durchführung oder Beendigung eines Bankgeschäfts erforderlich, an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Hierüber ist der Betroffene vor Abschluss eines Vertrags zu unterrichten (§ 28a Abs. 2 BDSG). Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf nach den Voraussetzungen des § 28 b BDSG ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden (sog. Scoring). Die Datenerhebung und Speicherung zum Zweck der Übermittlung bei der Auskunftei selbst richtet sich nach § 29 BDSG.

Folgende Fragen und Beschwerden waren vom TLfDI im Berichtszeitraum zu beantworten:

Wie lange dürfen Auskunfteien die Daten speichern?
Ein Betroffener, der nach einer Privatinsolvenz von der Restschuld befreit war, wandte sich an den TLfDI, weil seine Daten offenbar bei Auskunfteien weiterhin gespeichert waren. Er erhielt nämlich keine Ware ohne Vorkasse. Die Frage, wie lange dieser Zustand andauern sollte, hat der TLfDI unter Zugrundelegung des Wortlauts des einschlägigen § 35 Abs. 2 Nr. 4 BDSG beantwortet, weil die Daten geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden. Es ist am Ende des vierten Kalenderjahres, beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, zu löschen, wenn eine Prüfung ergibt, dass die Speicherung nicht mehr erforderlich ist. Soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widersprochen hat, beträgt diese Frist

drei Jahre. Das klingt zunächst kompliziert. Der Webseite der Schufa ist zu entnehmen, dass Informationen über die Eröffnung eines Verbraucherinsolvenzverfahrens bis zu sechs Kalenderjahren gespeichert werden. Gelöscht werden Informationen über die Erteilung einer Restschuldbefreiung nach drei vollen Kalenderjahren. Ebenso gelöscht werden die Daten über die Aufhebung eines Insolvenzverfahrens nach drei Jahren zum Jahresende. Um den konkreten Stand genau erfahren zu können, steht einem Betroffenen nach § 34 BDSG das Recht zu, von Auskunfteien einmal jährlich kostenlos eine Übersicht über die zur eigenen Person gespeicherten Daten zu verlangen. Sollte sich ergeben, dass in unzulässiger Weise Daten, die bereits gelöscht hätten sein müssen, weiterhin gespeichert werden, kann man sich an die Datenschutzaufsichtsbehörde wenden, die für die jeweilige Auskunftei zuständig ist. Mit diesen Informationen war der Betroffene offenbar zufrieden. Er hat sich beim TLfDI nicht mehr gemeldet.

Was ist, wenn eine falsche Auskunft vorliegt?

Weiterhin erreichte den TLfDI eine Beschwerde wegen einer Auskunftei-Datenübermittlung und unzulässiger Einholung von personenbezogenen Daten über eine Auskunftei von einem Inkassounternehmen in Thüringen. Die davon betroffene Person hatte den Schufa-Verbraucherservice in Anspruch genommen. Über diesen Verbraucherservice wurde sie darüber informiert, dass ein Inkassounternehmen aus Thüringen eine Anfrage zu Daten ihrer Person gestellt hatte. Laut eigener Recherchen der Schufa habe es sich hierbei um ein Versehen des Inkassounternehmens gehandelt. Dies mochte die betroffene Person aber nicht glauben. Die Geschäftsführerin des Inkassounternehmens sei nämlich früher bei demselben Unternehmen wie die Beschwerdeführerin beschäftigt gewesen. Daher könnten auch aus persönlichen Gründen Informationen gesammelt worden sein. Also forderte die Beschwerdeführerin das Inkassounternehmen auf, ihr mitzuteilen, welche personenbezogenen Daten über sie gespeichert sind. Postwendend bekam sie ein Formular, das sie zur Selbstauskunft nach § 34 BDSG ausfüllen und dem sie eine Personalausweiskopie mit Vorder- und Rückseite oder Reisepasskopie und Meldebescheinigung beifügen sollte. Darin sah die Beschwerdeführerin einen möglichen weiteren Vorstoß des Inkassounternehmens, Daten über sie zu erheben.

Auf Nachfrage des TLfDI erklärte das Inkassounternehmen den Ablauf im vorliegenden Fall. Zur Überprüfung und Verifizierung der im Internet über soziale Netzwerke recherchierten Adresse eines Schuldners mit ähnlich klingendem Namen sei eine Anfrage bei der Schufa gestellt worden. Daraufhin sei die Adresse der Beschwerdeführerin übermittelt worden. Eine Falschzuordnung, nämlich, dass es sich gar nicht um die tatsächlich gemeinte Schuldnerin handelte, war erst später bemerkt worden, denn es gab keinen Bezug zu der konkreten offenen Forderung, die eingetrieben werden sollte. Eine automatisierte Verarbeitung der bei der Auskunftei abgefragten personenbezogenen Daten sei nicht erfolgt, insoweit seien auch die Daten der Beschwerdeführerin beim Inkassounternehmen nicht gespeichert. Das Inkassounternehmen beabsichtigte zunächst, der Beschwerdeführerin mitzuteilen, dass keine zu ihrer Person gespeicherten Daten vorhanden seien. Das wäre aber inhaltlich nicht richtig gewesen. Immerhin hatte sich die Betroffene beschwert, sodass zumindest diese personenbezogenen Daten selbstverständlich zur Beantwortung verarbeitet und damit auch gespeichert wurden.

Zur Vorgehensweise des Inkassounternehmens konnte im Ergebnis der datenschutzrechtlichen Prüfung kein datenschutzrechtlicher Verstoß festgestellt werden. Nach § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Nachdem eine Forderung gegen eine Person mit zumindest ähnlichem Namen vorlag, konnten zur Adressfeststellung weitere Recherchen durchgeführt werden. Nachgewiesenermaßen erfolgte seitens des Inkassounternehmens zunächst eine Recherche in öffentlich zugänglichen sozialen Netzwerken. Eine besondere Schutzwürdigkeit der dort recherchierbaren Daten liegt aufgrund der öffentlichen Zugänglichkeit nicht vor.

Wie der Datenschutzbeauftragte der Schufa bestätigt hat, war das Auskunftsbegehren an die Schufa zur Verifizierung der Adresse einer Schuldnerin bzw. eines Schuldners nachvollziehbar und das berechtigte Interesse an den Auskünften gegeben.

Die beabsichtigte unrichtige Auskunft an die Beschwerdeführerin, nämlich dass keinerlei Datenspeicherungen vorlägen, hat die Beschwerdeführerin nicht erreicht. Weil die Post nicht zustellbar war, konnte das Inkassounternehmen letztendlich seiner Verpflichtung zur

Auskunft nicht nachkommen. Daher erhielt die Beschwerdeführerin das Ergebnis der datenschutzrechtlichen Prüfung einschließlich der Auskunft über die zu ihr beim Inkassounternehmen gespeicherten Daten vom TLfDI.
Zur Problematik des Verlangens einer Kopie des Personalausweises gilt, dass dies nach den gesetzlichen Vorschriften des Personalausweisgesetzes grundsätzlich unzulässig ist (siehe auch Nummer 2.26). Jedoch bedarf es einer Identitätsprüfung zum Zweck der Selbstauskunft nach § 34 BDSG, damit keinem Unbefugten Auskünfte über dritte Personen erteilt werden. Dazu muss der Personalausweis nicht kopiert werden. Der Nachweis der Identität kann auch mittels Vorlage und Einsicht in ein Ausweispapier erbracht werden. Dies bedingt jedoch, dass der Betroffene, der eine Selbstauskunft begehrt, persönlich vorstellig wird. Ist ihm dies nicht möglich oder zu beschwerlich, kann der Betroffene ersatzweise eine Kopie seines Identitätsnachweises übersenden, aus dem lediglich die erforderlichen zu überprüfenden Angaben wie Vor- und Zuname, vollständige Adresse, Geburtsdatum und Geburtsort erkennbar sind. Alle weiteren Angaben auf dem Ausweisdokument sind nicht erforderlich und können ggf. auf einer Kopie geschwärzt werden. Das betroffene Inkassounternehmen hat diesen Hinweis auf dem Formular zur Selbstauskunft nach § 34 BDSG nunmehr umgesetzt.

Auskunfteien verarbeiten personenbezogene Daten über Schuldner zu gemeldeten Forderungen, und diese Daten können auch zur Nachprüfung von Adressdaten genutzt werden. Betroffene haben nach § 34 BDSG das Recht, einmal jährlich kostenlos eine Übersicht über die zur eigenen Person gespeicherten Daten zu verlangen. Sollte sich ergeben, dass unzulässigerweise Daten gespeichert werden, kann man sich an die Datenschutzaufsichtsbehörde wenden, die für die jeweilige Auskunftei zuständig ist.

7.3 Einsichtsrechte nur bei berechtigtem Interesse

Das Grundbuch ist ein Register, in welches nicht jeder Einsicht nehmen darf. Er muss schon ein „berechtigtes Interesse“ haben. Ein berechtigtes Interesse liegt schon immer dann vor, wenn es sich aus vernünftigen Überlegungen ergibt und die vorgesehene Datenverwendung und der damit verfolgte Zweck im Einklang mit der

Rechtsordnung stehen. In diesem Rahmen kommen sowohl ideelle als auch wirtschaftliche Interessen in Betracht.
Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Beschwerde über eine unzulässige Weiterleitung von Grundbuch- und Katasterauszügen durch einen Notar an einen Immobilienmakler ein. Im Zusammenhang mit einem beabsichtigten Verkauf eines Grundstücks beauftragte ein Ehepaar einen Immobilienmakler per Maklervertrag. Noch vor Abschluss des Maklervertrages, erhielt das Ehepaar die erste Rechnung für einen vom Makler beigebrachten Grundbuchauszug. Weitere Rechnungen für einen unbeglaubigten Grundbuchauszug und einen Katasterauszug folgten. Die Eheleute hatten nach ihrer Aussage den Makler zu keinem Zeitpunkt mit der Einholung eines solchen Grundbuch- oder Katasterauszuges beauftragt bzw. bevollmächtigt. Insoweit hatten die Eheleute gegenüber dem TLfDI die Vermutung geäußert, der Makler hätte mit einem befreundeten Notar zusammen gearbeitet, welcher ihm die notwendigen Grundbuchauszüge beschafft hatte.
Der TLfDI hat hierzu umfassende Recherchen angestellt und neben dem Notar sowohl das örtliche Grundbuchamt, das Landesamt für Vermessung und Geoinformation, welches die zuständige Stelle für die Katasterauszüge ist, als auch das Thüringer Oberlandesgericht, in seiner Funktion als zuständige Stelle für das automatisierte Grundbuchabrufverfahren, um Stellungnahme zum Vorfall gebeten. Das Grundbuchamt teilte auf entsprechende Anfrage des TLfDI mit, dass der Notar im automatisierten Abrufverfahren nach § 133 Grundbuchordnung (GBO) Grundbuchauszüge abgerufen und ausgedruckt hatte. Mit dem § 133 a GBO (Erteilung von Grundbuchabdrucken durch Notare; Verordnungsermächtigung) hat der Gesetzgeber eine rechtliche Grundlage für die Notare geschaffen. Danach dürfen Notare demjenigen, der ihnen ein berechtigtes Interesse im Sinne des § 12 GBO darlegt, den Inhalt des Grundbuchs mitteilen. Die Mitteilung kann auch durch die Erteilung eines Grundbuchabdrucks erfolgen.
Die Erteilung von Katasterauszügen basiert auf Grundlage des § 18 Abs. 1 Thüringer Vermessungs- und Geoinformationsgesetz (ThürVermGeoG). Danach kann jede Person oder Stelle grundsätzlich die Datenbanken des amtlichen Vermessungswesens einsehen sowie Auskünfte daraus erhalten. Nach § 18 Abs. 2 ThürVermGeoG stehen abweichend von Abs. 1 die Einsicht in die Namen, die Ge-

burtsdaten und die Anschriften sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben und soweit überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Entsprechendes gilt für die Daten der Bevollmächtigten. Das berechtigte Interesse ist darzulegen. Die Empfänger dürfen diese Daten nur für den Zweck nutzen, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden.
Der TLfDI kam nach datenschutzrechtlicher Prüfung zu dem Ergebnis, dass die von dem Notar dargelegte Vorgehensweise datenschutzrechtlich unbedenklich war. Ausschlaggebend dafür war, dass zwischen dem Ehepaar und dem Immobilienmakler ein unterschriebener Makler-Allein-Auftrag vorlag. In diesem Makler-Allein-Auftrag hatte das Ehepaar dem Immobilienmakler eine Vollmacht zur Grundbucheinsicht und in die Grundakte sowie in alle übrigen in Frage kommenden behördlichen Akten erteilt. Durch Vorlage des von dem Ehepaar unterschriebenen Makler-Allein-Auftrages hat der Notar das berechtigte Interesse zur Erteilung eines Grundbuchabdruckes an den Immobilienmakler einwandfrei nachgewiesen.
Im Ergebnis war aufgrund ordnungsgemäßer Bevollmächtigung sowohl das Abrufen des Grundbuchauszuges als auch das des Katasterauszuges durch gesetzliche Grundlagen gerechtfertigt.

Nach § 133a GBO dürfen Notare demjenigen, der ihnen ein berechtigtes Interesse im Sinne des § 12 darlegt, den Inhalt des Grundbuchs mitteilen. Die Mitteilung kann auch durch die Erteilung eines Grundbuchabdrucks erfolgen. Die Erteilung von Katasterauszügen basiert auf Grundlage des § 18 Abs. 1 Thüringer Vermessungs- und Geoinformationsgesetz (ThürVermGeoG). Danach kann jede Person oder Stelle grundsätzlich die Datenbanken des amtlichen Vermessungswesens einsehen sowie Auskünfte daraus erhalten. Nach Abs. 2 steht die Einsicht in die Namen, die Geburtsdaten und die Anschriften sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben und soweit überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Ein unterschriebener Makler-Allein-Auftrag stellt ein berechtigtes Interesse dar.

7.4 Auskunfteien: datenschutzrechtlicher Quell der "Freude" – Fortsetzung 1

Können Auskunfteien eine Selbstauskunft nach § 34 Bundesdatenschutzgesetz (BDSG) ablehnen?

Ein Meldeamt wies einen Betroffenen darauf hin, dass eine Wirtschaftsauskunftei in Thüringen eine erweiterte Melderegisterauskunft zu seiner Person erfragt habe. Auf Nachfrage nach den Hintergründen erhielt er von der Wirtschaftsauskunftei die Antwort, die Datenspeicherung sei nach § 29 Bundesdatenschutzgesetz (BDSG) erlaubt, wenn kein Grund zu der Annahme bestehe, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Speicherung habe. Nach dieser Vorschrift sei es auch zulässig, die Daten zu übermitteln, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlege. Weder zur Speicherung noch zur Übermittlung sei nach Auffassung der Wirtschaftsauskunftei eine Genehmigung erforderlich. Bis dahin ist alles richtig. Allerdings bat die Wirtschaftsauskunftei dann um das Verständnis des Betroffenen, dass sie den Anfragegrund leider nicht offenlegen könne. Sie sei nämlich ihrem Auftraggeber gegenüber zur Diskretion verpflichtet. Verständlich, dass sich der Beschwerdeführer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als Aufsichtsbehörde wandte, der die Sache überprüfte.

Die Auskunftei schilderte dem TLfDI den Verfahrensablauf: Eines ihrer Mitgliedsunternehmen habe aus plausiblem Grund zu dem Betroffenen angefragt. Da bis dahin über den Betroffenen bei der Auskunftei noch nichts bekannt war, habe man – wie üblich – recherchiert. Es sei nichts bekannt gewesen, was gegen eine Datenerhebung bzw. eine Beauskunftung an das Mitgliedsunternehmen sprechen könnte. Also habe man Informationen recherchiert, den Datensatz gespeichert und die Auskunft erteilt. Die erweiterte Meldeauskunft habe man gegenüber der Meldebehörde damit begründet, dass das Mitgliedsunternehmen eine Bonitätsauskunft benötige, um ein kreditorisches Geschäft abzusichern. Gegen den geschilderten Ablauf bestehen grundsätzlich keine datenschutzrechtlichen Bedenken.

Die Begründung allerdings dafür, dass dem Betroffenen aus Gründen der Diskretion keine Auskunft gegeben werden könne, war inakzeptabel. Nach der Darlegung der Auskunftei war dem anfragenden Mitgliedsunternehmen zugesichert worden, Auskunftsbegehren ge-

genüber den Betroffenen nicht offenzulegen. Aus geschäftspolitischen Gründen sollte verhindert werden, dass der Betroffene erfährt, dass zu ihm eine Bonitätsauskunft bei einer Auskunftei eingeholt wird oder worden ist. Die Auskunftseinholung führe in der Praxis nämlich immer wieder zu Vertrauensverlusten und damit zu Gefährdungen der Geschäftsbeziehungen.
Der TLfDI wies darauf hin, dass diese allgemeine Befürchtung und pauschale Zusage, dem Betroffenen keine Auskunft über die Bonitätsauskunftsempfänger zu erteilen, im Hinblick auf die eindeutige Regelung des § 34 Abs. 1 Satz 4 BDSG nicht ausreiche. Die Auskunft über die Empfänger kann nach den gesetzlichen Vorschriften nur dann verweigert werden, wenn das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt, § 34 Abs. 1 Satz 3 BDSG. Demnach ist immer eine Abwägung im Einzelfall notwendig. Im Zweifel muss die Auskunftei den Empfänger der Bonitätsauskunft zur Klärung der Frage einbeziehen, welche konkreten Gründe vorliegen, die das Informationsinteresse des Betroffenen überwiegen könnten. Hier wurde aber offensichtlich nur das pauschale Interesse des Mitgliedsunternehmens an der Heimlichkeit berücksichtigt. Das reicht keinesfalls aus. Der TLfDI hat die Auskunftei aufgefordert, die begehrte Auskunft an den Betroffenen zu erteilen. Dem ist sie letztendlich nachgekommen. Also erhielt der Betroffene die Auskunft, welches Unternehmen denn die erweiterte Melderegisterauskunft veranlasst hatte. Ob dies dem Vertrauen zu dem Unternehmen geschadet hat, ist nicht bekannt geworden.

Sind Auskunfteien immer die Bösen?
Ein weiterer Beschwerdeführer wandte sich an den TLfDI, weil ein Thüringer Inkassounternehmen der Schufa die Forderung eines Versandhauses gemeldet habe, die nach seiner Buchführung längst beglichen sei. Der Betroffene berief sich auf ein Aktenzeichen der Schufa, unter dem er hierüber Auskunft erhalten habe, und beklagte sich, er habe von dem Inkassounternehmen auf seine Anfragen überhaupt keine Antwort erhalten. Da nach dem Vorbringen keine offene Forderung vorlag, die die Voraussetzung zur Übermittlung an die Schufa nach § 28 a BDSG erfüllt hätte, schrieb der TLfDI als Aufsichtsbehörde das Inkassounterunternehmen an. Dieses erklärte, es sei weder Mitglied der Schufa, noch habe es der Schufa Daten zu dem Betroffenen gemeldet. Es wies jegliche Unterstellungen weit

von sich und verlangte „behauptungsunterlegende Beweise“. Der Bitte, dem TLfDI für eine konkrete weitergehende Überprüfung belegende Unterlagen zur Verfügung zu stellen, kam der Beschwerdeführer nicht nach, weswegen eine tiefergehende Prüfung bisher nicht möglich war.

Auskünfte an einen Betroffenen über den Zweck der Speicherung seiner Daten, deren Herkunft sowie über den anfragenden Empfänger können nach § 34 BDSG nicht verweigert werden, weil einem Mitgliedsunternehmen „Diskretion“ zugesagt wurde. Für eine datenschutzrechtliche Prüfung benötigt der TLfDI in Zweifelsfällen belastbare Unterlagen, um helfen zu können.

7.5 Auskunfteien: datenschutzrechtlicher Quell der "Freude" – Fortsetzung 2 – Stichprobenverfahren zur Prüfung des berechtigten Abrufinteresses

Nach § 29 Abs. 2 Satz 5 Bundesdatenschutzgesetz (BDSG) haben Wirtschaftsauskunfteien das Vorliegen eines berechtigten Interesses zu Auskunftsabfragen im Stichprobenverfahren einzelfallbezogen festzustellen und zu überprüfen. Hierzu werden ausgewählte Auskunftsempfänger zu näheren Erläuterungen und entsprechenden Nachweisen aufgefordert. Die Datenschutzaufsichtsbehörden sind sich darüber einig, dass jedenfalls dann, wenn als Nachweis geeignete Unterlagen vorhanden sind, diese durch den Auskunftsempfänger (in Kopie) auch vorzulegen sind.
In der Praxis gibt es immer wieder Probleme dahingehend, dass Auskunftsempfänger die Vorlage von Unterlagen aus „Datenschutzgründen“ verweigern und damit eine Prüfung des berechtigten Interesses durch die Wirtschaftsauskunftei verhindern. So auch ein Thüringer Personaldienstleister, der nach dem Vorbringen einer Wirtschaftsauskunftei in einem anderen Bundesland partout der Begründung des berechtigten Interesses nicht nachkommen wollte. Die Wirtschaftsauskunftei wandte sich an die dortige Aufsichtsbehörde, die dem Thüringer Landesbeauftragten für den Datenschutz und Informationsfreiheit (TLfDI) zuständigkeitshalber die Prüfung anheimstellte.
Auf Anfrage des TLfDI teilte der Personaldienstleister mit, er wolle seiner Verpflichtung gerne nachkommen, sofern ihm mitgeteilt werde, auf welche konkreten Auskünfte sich die vorzulegenden Unterla-

gen denn bezögen. Auch habe er keine Anfragen an die Wirtschaftsauskunftei in dem anderen Bundesland gerichtet, sondern lediglich an eine Auskunftei in Thüringen. Von dort sei ihm im Übrigen bestätigt worden, dass er jeweils der Vorlage von angeforderten Unterlagen nachgekommen sei.
Der TLfDI muss den Sachverhalt also weiter aufklären.

Das berechtigte Interesse an einer Auskunftsabfrage ist von Wirtschaftsauskunfteien nach § 29 Abs. 2 Satz 5 BDSG in einem Stichprobenverfahren zu überprüfen. Die Abfragenden haben hierzu Nachweise vorzulegen.

7.6 Bei Online-Bestellung zuerst Auskunfteien-Abfrage

Der Internethandel ist eine feine Sache. Zuhause das Angebot am Bildschirm durchstöbern, bei Gefallen ab in den Warenkorb, Bezahlart „Rechnung“ wählen und kurz darauf klingelt der Paketdienst. Sofern sich keine Gründe für einen Umtausch der Ware ergeben, wird der Kaufpreis überwiesen. So hatten es sich auch mehrere Beschwerdeführer vorgestellt. Was sie nicht einkalkuliert hatten, war, dass über sie erstmal eine Abfrage bei Auskunfteien eingeholt wird, denn der Händler will ja letztendlich selbstverständlich auch sein Geld sehen und nicht erst klagen und vollstrecken müssen.
Ein Betroffener hatte bei seiner Internetbestellung bei einem Thüringer Unternehmen (im weiteren „Verkäufer“) erstmal „Kauf auf Rechnung“ angeklickt. Nach einer Bonitätsprüfung mittels Auskunftei-Abfrage durch den Verkäufer wurde die Zahlungsart vom Verkäufer auf „Vorkasse“ geändert. Auf seine Nachfrage wurde ihm vom Verkäufer mitgeteilt, man habe Daten bei einer näher bezeichneten, nicht im Zuständigkeitsbereich des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ansässigen Auskunftei abgerufen. Aufgrund des dabei mitgeteilten Prüfwerts (Scorewert – § 28b Bundesdatenschutzgesetz [BDSG]), der „aus datenschutzrechtlichen Gründen“ nicht mitgeteilt werden könne, gäbe es keinen Kauf auf Rechnung. Zu näheren Einzelheiten solle sich der Betroffene direkt an die Auskunftei wenden, die unter einer angegebenen Telefon- oder Faxnummer erreichbar sei. Also wandte sich der Betroffene an den TLfDI als zuständige Datenschutzaufsicht für in Thüringen ansässige Unternehmen, da er davon

ausging, dass ihm der Verkäufer doch mitteilen müsse, was er über ihn gespeichert habe.
Der TLfDI wandte sich unter Darlegung folgender Rechtsauffassung an den Verkäufer: Die über den Betroffenen bei den Auskunfteien nach § 28b BDSG eingeholten Auskünfte unterliegen einer vom Gesetzgeber ausdrücklich geregelten Auskunftspflicht, § 34 Abs. 2 BDSG. In § 34 Abs. 2 Satz 4 BDSG wird die Möglichkeit eingeräumt, den Betroffenen an die Stelle zu verweisen, die den Wahrscheinlichkeitswert (Scorewert) berechnet hat (Auskunftei). Diese Verweisungsmöglichkeit an die Auskunftei ist aber an kumulativ vorliegende Voraussetzungen gebunden. Der Scorewert muss eigenständig von der Auskunftei berechnet worden sein. Die Verweisung muss unverzüglich unter Nennung von Name und Anschrift der Auskunftei sowie aller Informationen, die zur Bezeichnung des Einzelfalls gegenüber der Auskunftei notwendig sind, erfolgen.
Jedenfalls war der Betroffene nicht über Name und Anschrift der Auskunftei informiert worden. Diese Angaben waren zwar in den Allgemeinen Geschäftsbedingungen (AGB) des Verkäufers enthalten, der Verweis auf das „Kleingedruckte“ reicht allerdings in diesem Zusammenhang nicht aus. Ebenfalls beinhaltete die Auskunft an den Betroffenen keinerlei Angaben, wie z. B. ein Aktenzeichen oder eine Geschäftsgangbezeichnung, die es dem Betroffenen ermöglichen würde, sich in seiner Anfrage an die Auskunftei auf die konkrete Anfrage zu beziehen. Es blieb daher bei dem in § 34 Abs. 2 Satz 1 BDSG normiertem Auskunftsrecht gegenüber dem Verkäufer.
Daraufhin hat der Verkäufer erstmal die komplette Anschrift der Auskunftei in das Muster des Kundenanschreibens eingearbeitet und glaubte so, seiner Verpflichtung nachgekommen zu sein.
Da zwischenzeitlich weitere Beschwerden beim TLfDI eingegangen waren, weil Betroffene nach dem Musterschreiben einfach auf die Auskunftei verwiesen wurden, wurde gegenüber dem Verkäufer nochmals deutlich gemacht, dass auch er verpflichtet ist, Auskünfte über die in seinem Unternehmen verarbeiteten Kundendaten zu erteilen. Es reicht in diesen Fällen nicht aus, die Betroffenen lediglich darauf hinzuweisen, dass Adressdaten gespeichert sind und für alles Weitere auf die Auskunftei verwiesen wird. Das die Bonität abfragende Unternehmen kann sich nicht darauf zurückziehen, die Betroffenen an eine Auskunftei, bei der es Auskünfte eingeholt hat zu verweisen, wenn es diese Auskünfte für Geschäftszwecke weiterhin selbst speichert.

Nun rückte der Verkäufer mit der Information heraus, dass, sofern Scorewerte von Auskunfteien bezogen würden, diese nach der Entscheidung über den Geschäftsabschluss gelöscht würden. Daher könnten die Betroffenen von ihm hierüber auch keine Auskunft erhalten. Hierauf würden die Betroffenen zukünftig hingewiesen.
Weiterhin ist es aus Sicht des TLfDI selbstverständlich, dass Onlinekäufer vor Auswahl einer Bezahlmöglichkeit die Information erhalten müssen, dass bei Auswahl des Kaufs auf Rechnung (einer sog. unsicheren Zahlungsart) eine Bonitätsabfrage bei Auskunfteien erfolgt. Lediglich ein Hinweis darauf in den AGB reicht für eine wirksame Einwilligung zur Abfrage bei Auskunfteien nicht aus. Der Käufer muss für seine Entscheidung, dass mit Auswahl des „auf Rechnung“ auch eine Abfrage bei einer Auskunftei verbunden ist oder sein kann, ausreichend informiert sein. Der TLfDI wird diesen Aspekt in seine zukünftige Prüftätigkeit einbeziehen.

Onlinehändler müssen den Käufern auf deren Nachfrage mitteilen, welche personenbezogenen Daten sie über ihn speichern. Wurden Auskünfte eingeholt, sind dem Betroffenen die genaue Bezeichnung und die Adresse der Auskunftei sowie ein Aktenzeichen mitzuteilen, damit er der Auskunftei gegenüber sein Auskunftsrecht wahrnehmen kann. Bei der Auswahl der Zahlungsart muss der Käufer wissen, ob eine bestimmte Art eine Abfrage bei einer Auskunftei voraussetzt.

7.7 Kostenlose Schufa-Selbstauskunft: so geht´s

Seit dem 1. April 2010 ist die Schufa per Gesetz dazu verpflichtet, jedem Bürger einmal jährlich auf Nachfrage eine Schufa-Selbstauskunft zu erteilen – und zwar kostenlos (§ 34 Bundesdatenschutzgesetz – BDSG). Jede weitere Auskunft ist kostenpflichtig. Die kostenlose Selbstauskunft ist allerdings auf der Website der Schufa etwas versteckt. Da die Schufa ihren Sitz in Hessen hat, kann der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) allerdings keinen direkten Einfluss auf eine benutzerfreundlichere Gestaltung nehmen.

So sollten Sie vorgehen: Rufen Sie zuerst die Startseite der Schufa auf (www.schufa.de). Klicken Sie dann oben

auf "Privatkunden". An dieser Stelle haben Sie die Möglichkeit, die Online-Auskunft zu erfragen – allerdings gegen Gebühr. Für die kostenfreie Auskunft klicken Sie stattdessen auf dieser Seite ganz oben links auf "Auskünfte". Anschließend klicken Sie links auf den Menüeintrag "Datenübersicht nach § 34 Bundesdatenschutzgesetz". Klicken Sie auf den Button "Jetzt bestellen" unter dem Eintrag "Datenübersicht nach § 34 BDSG". Nun muss noch auf die Flagge der Sprache geklickt werden, in welcher Sie das Formular ausfüllen möchten. Es öffnet sich ein PDF-Formular, das Sie ausdrucken, ausfüllen und an die Schufa senden müssen. Auch auf dem ausgedruckten Formular erhalten Sie noch einmal die Möglichkeit, eine kostenpflichtige Schufa-Selbstauskunft einzuholen. Dieses Feld müssen Sie leer lassen. Als Anlage zu dem Formular finden Sie weitere Auskünfte, wie zu verfahren ist.

Nach § 34 Abs. 8 BDSG haben Betroffene das Recht, einmal jährlich auf Antrag eine kostenlose Schufa-Selbstauskunft zu erhalten.

7.8 Auskunft – sonst ... Die Zweite!

Ein Betroffener beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Unternehmen ihn nach Aufforderung und Fristsetzung nicht über die zum Betroffenen dort gespeicherten personenbezogenen Daten informierte.
Nach § 34 Bundesdatenschutzgesetz (BDSG) ist die verantwortliche Stelle, also das Unternehmen, welches die personenbezogenen Daten gespeichert hat, verpflichtet, dem Betroffenen auf Verlangen darüber Auskunft zu erteilen, welche Daten sie über den Betroffenen gespeichert hat, woher diese kamen und an wen diese weitergegeben wurden. Ebenfalls hat das Unternehmen über den Zweck der Speicherung Auskunft zu erteilen.
Wird eine solche Auskunft übrigens nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt, kann dies mit einer Geldbuße von bis zu 50.000 Euro geahndet werden, § 43 Abs. 1 Nr. 8a BDSG.
Im hiesigen Fall hat der TLfDI die verantwortliche Stelle angeschrieben und über ihre Pflichten belehrt. Daraufhin wurde die verlangte Auskunft an den Betroffenen erteilt.

Verantwortliche Stellen sind verpflichtet, Auskunft über die zur Person gespeicherten Daten zu erteilen. Dieser Auskunftsanspruch bezieht sich auch auf Daten zur Person aus Videoaufnahmen.
Als Betroffener ist es immer ratsam, der verantwortlichen Stelle eine Frist zur Beantwortung zu setzen und eine Art und Weise der Zustellung zu wählen, mit der der Zugang des Schreibens nachweisbar ist. Kommt man nicht weiter: TLfDI einschalten!

Stressed spam – © alphaspirit / Fotolia.com

8 Werbung

8.1 Payback-Karte: Sie zahlen mit Ihren Daten – aber nur bei gültiger Einwilligung

Wer kennt das nicht: Sie stehen an der Kasse und werden mit den Fragen konfrontiert: "Haben Sie eine Kundekarte?", "Haben Sie eine Payback-Karte?" oder "Sammeln Sie Marken oder Punkte?". Dies ist nichts Neues. Solche Kundenkarten gehören im Handel mittlerweile zum Standardrepertoire. Vom Supermarkt über die Drogerie bis zur kleinen Bäckerei bieten fast alle Betriebe ihren Kunden die Treue-Ausweise an, die meist mit Vorteilen – etwa Sonderangeboten – verbunden sind. Die Schattenseite der Karten ist der oft mangelnde

Datenschutz. Neben dem Weiterverkauf der Kundendaten, wenn der Kunde im Kartenantrag der „Erlaubnis zur weitergehenden Verwendung der gespeicherten Daten“ nicht widerspricht, besteht auch die Gefahr, dass Dritte sich beim Verlust der Karten Zugang zu den Daten des Inhabers verschaffen.

Erfreulicherweise meldete sich eine solche Kundin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Kundin eines großen Einzelhandelsunternehmens hatte gerade eine Kundenkarte beantragt. Dabei erhob das Unternehmen für den Kartenantrag Name, Anschrift, Geburtsdatum sowie ihre Unterschrift. Die Kundin stellte daraufhin entsetzt fest, dass das Unternehmen die auf einem Tablet erfassten Daten als unverschlüsselte Mail – zumindest an sie selbst – weitergeleitet hatte. Das Unternehmen hatte sogar die elektronische Unterschrift (Pen Pad) der Kundin weitergeleitet. Im Anschluss daran erkundigte sich die Kundin beim TLfDI, ob diese Vorgehensweise datenschutzrechtlich zulässig ist.

Für einen Kundenkartenantrag ist eine Einwilligung in die Verwendung der personenbezogenen Daten von den Kunden regelmäßig notwendig, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Nach § 4a Abs. 1 Satz 2 BDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das Gesetz räumt zwar der Schriftform den unbedingten Vorrang ein, gibt aber einer anderen Form den Vorrang, wenn besondere Umstände dieses rechtfertigen. Weder eine konkludente noch eine stillschweigende oder gar mutmaßliche Einwilligung reichen infolgedessen aus. Wann besondere Umstände im Sinne des Gesetzes vorliegen, lässt sich nicht abstrakt sagen, sondern nur in Kenntnis der spezifischen Verarbeitungsumstände.

Gerade mit der Vorgehensweise mittels eines Pen Pads konnte das Unternehmen nicht das Schriftformerfordernis im Sinne des BDSG wahren. Bei solch einem Pen Pad handelt es sich um ein Gerät, mit dem eine eigenhändige Unterschrift elektronisch erfasst wird. In Kombination mit digitalen Signaturen dienen elektronisch erfasste Unterschriften dazu, elektronische Dokumente zu unterzeichnen bzw. zu signieren, um so einen Medienbruch vom elektronischen zum Papierdokument und zurück zu vermeiden.

Nach § 4a BDSG kann die Einwilligung auch in elektronischer Form abgegeben werden. Das Bundesdatenschutzgesetz geht im Gesetzestext nicht auf die Möglichkeit einer elektronischen Einwilligung ein.

Einer ausdrücklichen Erwähnung bedarf dies allerdings nicht. Die elektronische Form ist vielmehr so lange zulässig, wie sie nicht eindeutig ausgeschlossen wird, § 126 Abs. 3 Bürgerliches Gesetzbuch (BGB). Solch eine Regelung fehlt im § 4a BDSG. Elektronische Einwilligungen können daher jederzeit anstelle der gesetzlich vorgesehenen schriftlichen Einverständniserklärungen verwendet werden (vergleiche Simitis, Kommentar zum Bundesdatenschutzgesetz, 8. Auflage, § 4, Rn. 36). Jedoch sind elektronische Einwilligungen nur unter bestimmten, in jedem Fall einzuhaltenden Bedingungen wirksam. Sie müssen nach § 126 a BGB nachweisbar von den Betroffenen vorgenommen worden sein, ihnen zugeordnet werden können und eine den Anforderungen des Signaturgesetzes (SigG) entsprechende digitale Signatur aufweisen.
Die „qualifizierte elektronische Signatur“ ist die einzige Art an elektronischer Signatur, die ein gesetzliches Schriftformerfordernis ersetzen kann und in Gerichtsverfahren als Beweismittel zugelassen ist. Deshalb gelten für sie die höchsten gesetzlichen Anforderungen. Neben den Merkmalen einer fortgeschrittenen elektronischen Signatur gemäß § 2 Nr. 2 SigG muss sie zwei zusätzliche Voraussetzungen erfüllen. Eine fortgeschrittene elektronische Signatur ist eine elektronische Signatur, die es ermöglicht, die Authentizität und Unverfälschtheit der durch sie signierten Daten zu prüfen. Die EG-Richtlinie 1999/93/EG („Signaturrichtlinie“) fordert für fortgeschrittene elektronische Signaturen, dass diese „ausschließlich dem Unterzeichner zugeordnet sind, die Identifizierung des Unterzeichners ermöglichen, mit Mitteln erzeugt werden, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann und mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann“. Bei der „qualifizierten elektronischen Signatur“ muss zusätzlich erstens die Signatur auf einem gültigen Zertifikat beruhen und zweitens mit einer sicheren Signaturerstellungseinheit erzeugt werden. Elektronische Einwilligungen, die diese Bedingungen nicht erfüllen, sind nichtig, wenn eben nicht andere besondere Umstände bestehen, die ein Abweichen von der Schriftform rechtfertigen.
Der TLfDI benötigt für eine abschließende Beurteilung der datenschutzrechtlichen Zulässigkeit des Vorgehens des Einzelhandelsunternehmens mittels eines Pen Pads von der Kundin jedoch weitere Informationen. Im hiesigen Fall konnte die Kundin den benötigten

Kundenkartenantrag und die übersandte E-Mail mittels Pen Pad nicht nachreichen. Das Verfahren ist noch nicht abgeschlossen.

Beim Abschluss eines Kundenkartenantrages ist eine Einwilligung der Kunden in die Verwendung der personenbezogenen Daten notwendig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, § 4a Abs. 1 Satz 2 BDSG. Elektronische Einwilligungen sind nur unter bestimmten, in jedem Fall einzuhaltenden Bedingungen wirksam. Sie müssen nachweisbar von den Betroffenen vorgenommen worden sein und ihnen zugeordnet werden können, sowie eine den Anforderungen des § 2 SigG entsprechende digitale Signatur aufweisen, § 126a BGB.

8.2 Datenschutzverletzung durch unzulässige Anwaltswerbung

Wenn Rechtsanwälte werben, gelten auch für sie die Regeln des Bundesdatenschutzgesetzes (BDSG). Halten sie diese nicht ein, und erfährt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, muss dieser einschreiten.
So auch in diesem Fall. Ein Anwalt vertrat einen Gläubiger in einem Insolvenzverfahren über eine Anlegergesellschaft. Nach Einsicht in die Insolvenzakte wandte er sich an sämtliche andere Gläubiger des insolventen Unternehmens und informierte diese über die rechtliche Situation. Soweit war dagegen auch nichts einzuwenden. Der Rechtsanwalt bzw. dessen Mandant hat ein Einsichtsrecht in die Insolvenzakte nach § 299 Zivilprozessordnung (ZPO). Auch darf der Rechtsanwalt zur Mandatsbearbeitung hieraus personenbezogene Daten erheben und verarbeiten. Insoweit prüft der TLfDI, wenn überhaupt, dann nur sehr eingeschränkt, da ein Rechtsanwalt hier als unabhängiges Organ der Rechtspflege einen sehr breiten Entscheidungsspielraum hat.
Eine Grenze wird allerdings überschritten, wenn der Rechtsanwalt dem Schreiben einen werblichen Charakter gibt, indem er ganz konkret bei sämtlichen anderen Gläubigern aus der Insolvenzakte zum Zwecke einer Mandatserteilung im Einzelfall wirbt und auch schon ein konkretes Angebot abgibt. Dann werden nämlich die nach§ 299 Abs. 1 ZPO zum Zwecke der Mandatsbearbeitung erhobenen Daten zweckwidrig zu Zwecken der Werbung genutzt.

Die Voraussetzungen für die Nutzung von personenbezogenen Daten sind abschließend in § 28 Abs. 3. BDSG geregelt. Grundsätzlich ist danach Werbung nur mit der Einwilligung der Beworbenen zulässig. Zwar gibt es hierzu umfassende Ausnahmen, aber auch diese sind an bestimmte Voraussetzungen gekoppelt. So ist nach § 28 Abs. 3 Satz 2 BDSG die Verarbeitung oder Nutzung personenbezogener Daten ohne Einwilligung dann zulässig, wenn es sich nur um so genannte Listendaten handelt, wie hier der Fall. Jedoch ist dabei § 28 Abs. 3 Satz 2 zweiter Halbsatz Ziffer 1–3 BDSG zu beachten. Die Verarbeitung oder Nutzung muss erforderlich sein für die Zwecke der Werbung, für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Abs. 1 Satz 1 Nr. 1 oder aus allgemein zugänglichen Adressrufnummern, Branchen oder vergleichbaren Verzeichnissen erhoben hat (Ziff. 1), für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Beworbenen und unter seiner beruflichen Anschrift (Ziff. 2) oder für Zwecke der Werbung für Spenden (Ziff. 3).
Eine Einwilligung der weiteren Betroffenen aus der Insolvenzakte lag hier nicht vor. Auch handelte es sich vorliegend nicht um allgemein zugängliche Daten aus Adressverzeichnissen oder Telefonbüchern. Weder nutze der Rechtsanwalt die Daten für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit der anderen Gläubiger des insolventen Unternehmens noch für Spenden. Die einzig wirklich naheliegende Alternative nach Ziff. 1. scheitert daran, dass es sich nicht um Daten handelt, die nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben worden sind, sondern nach § 299 Abs. 1 ZPO.
Im Ergebnis war das Anschreiben des Rechtsanwalts also datenschutzwidrig, da es einen werbenden Charakter hatte, aber gegen die hierfür geltenden Regelungen des BDSG verstieß.
Der TLfDI prüft den Erlass einer Anordnung.

Grundsätzlich ist die werbliche Ansprache unter Verwendung personenbezogener Daten (Adressdaten) nur mit Einwilligung des Beworbenen zulässig. Liegt eine solche nicht vor, müssen die Ausnahmen hierzu vorliegen.

8.3 Auskunft sonst ... Die Dritte!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt zum wiederholten Male eine Beschwerde über eine unterbliebene Auskunftserteilung gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG). Beschwert wurde sich über das gleiche Unternehmen wie aus dem Beitrag „Auskunft sonst …“ (siehe Beitrag Nummer 2.40). Anlass dieser Beschwerde war ebenfalls ein unerwünschter Werbeanruf. Der Beschwerdeführer sollte an einer Energiebefragung teilnehmen. Auf Nachfrage des Beschwerdeführers teilte dieses Unternehmen mit, dass der Beschwerdeführer seine Daten auf einer nicht existierenden Gewinnspielseite eingegeben hätte. Daher wollte er in seinem Auskunftsersuchen von dem Unternehmen wissen, welche Daten über ihn bei dem Unternehmen gespeichert waren und wo sie herkamen, an wen seine personenbezogenen Daten weitergegeben wurden und den Zweck der Speicherung seiner Daten bei dem Unternehmen erfahren. Aus dem Schutzzweck des § 34 Abs. 1 BDSG folgt, dass die Betroffenen eine schnelle Auskunftserteilung verlangen können. Je länger sie auf eine Auskunft warten müssen, desto größer ist das Risiko, dass aufgrund unrichtiger Daten u. U. nicht mehr rückgängig zu machende Entscheidungen zu deren Nachteil getroffen werden. Eine gesammelte Bearbeitung von Auskunftsersuchen der Unternehmen ist nur dann zulässig, wenn sie in kurzen Zeitabständen – innerhalb von ein bis zwei Wochen – beantwortet werden. Eine längere Frist zur Beantwortung eines Auskunftsersuchens nach § 34 Abs. 1 BDSG ist nur unter besonderen Umständen gerechtfertigt (Dix in Simitis, Kommentar BDSG, 8. Auflage, § 34, Rn. 42). In jedem Fall müssen aber die vom Betroffenen gesetzten Fristen, sofern diese angemessen sind, eingehalten werden. Hiervon ist bei einer 14-Tagesfrist in der Regel auszugehen. In diesem Fall wurde die Auskunft bis vier Monate nach dem Auskunftsersuchen des Beschwerdeführers seitens des Unternehmens nicht beantwortet.

Auch in dieser Sache wird der TLfDI dem Unternehmen die Auskunftserteilung anordnen. Darüber hinaus wird es aller Wahrscheinlichkeit nach zu einem Bußgeldverfahren kommen. Gemäß § 43 Abs. 1 Nr. 8a BDSG handelt ordnungswidrig, wer eine Auskunft nach § 34 Abs. 1 BDSG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. Bei der Bemessung der Geldbuße wird

dann auch berücksichtigt werden, dass das Unternehmen zum wiederholten Male eine Auskunftserteilung unterlassen hat.

Das Auskunftsrecht ist regelmäßig Voraussetzung für die Ausübung und damit selbst Bestandteil des Rechts auf informationelle Selbstbestimmung.

8.4 Wann ist das „Double-Opt-In"-Verfahren zulässig?

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass ein Unternehmen ihn nach Aufforderung und Fristsetzung nicht über seine gespeicherten personenbezogenen Daten informierte. Darüber hinaus hatte der Betroffene das Unternehmen um Information gebeten, an welche Dritten seine personenbezogenen Daten weitergegeben worden sind.
Nach § 34 Bundesdatenschutzgesetz (BDSG) ist die verantwortliche Stelle, also das Unternehmen, welches die personenbezogenen Daten gespeichert hat, verpflichtet, dem Betroffenen auf Verlangen darüber Auskunft zu erteilen, welche Daten dieses über den Betroffenen gespeichert hat, woher diese kamen und an wen diese weitergegeben wurden. Ebenfalls hat das Unternehmen über den Zweck der Speicherung Auskunft zu erteilen.
Im hiesigen Fall hat der TLfDI die verantwortliche Stelle angeschrieben und über ihre Pflichten belehrt. Daraufhin wurde die verlangte Auskunft an den Betroffenen erteilt. Nach Auskunft des Unternehmens stammten die personenbezogenen Daten aus einem Newslettereintrag, den der Betroffene bei dem Unternehmen vorgenommen und den dieser auch per „Double-Opt-In"-Verfahren bestätigt habe. Eine Weitergabe der Daten an Dritte sei nicht erfolgt.
Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, vergleiche § 4a Abs. 1 BDSG. Wer also einen Newsletter verschicken möchte, ist gesetzlich dazu verpflichtet, den Empfänger vorher um Erlaubnis zu fragen, vergleiche § 28 Abs. 3 Satz 1 BDSG. Nach § 28 Abs. 3 Satz 2 kann eine Verarbeitung oder Nutzung personenbezogener Daten zwar in bestimmten Fällen auch ohne Einwilligung

der Betroffenen erfolgen, sofern Angaben über Personen, die einer Gruppe angehören, in Listen oder sonst zusammengefasst und für Werbezwecke verwendet werden. Jedoch zählt gerade eine E-Mail-Adresse nicht zu den „Listendaten“. Es bleibt daher bei der Voraussetzung der Einwilligung.
Für das elektronische Erklären einer Einwilligung ist – zur Verifizierung der Willenserklärung des Betroffenen – das „Double-Opt-In“-Verfahren geboten. Bei einem „Double-Opt-in“-Verfahren erhält ein Nutzer, der sich im ersten Schritt mit seiner E-Mail-Adresse in einen Verteiler eingetragen hat (Single-Opt-In), im zweiten Schritt durch eine anschließende Bestätigungs-E-Mail die Möglichkeit, die Anmeldung zu bestätigen. Diese Nachricht wird auch als "DOI" oder "DOI-Mail" bezeichnet. Handelt es sich um ein echtes, das heißt erwünschtes Opt-In, bekommt der Abonnent eine Bestätigung seiner angegebenen Kontaktdaten. Handelt es sich dagegen um einen missbräuchlich, also ohne Einwilligung erfolgten Eintrag, kann sich der unfreiwillige Abonnement-Kandidat vor einem Eintrag in die Abonnementliste schützen, indem er auf die Bestätigungsanfrage nicht reagiert. Er hat dabei immer die Möglichkeit, das Mailing-Abo zu stornieren. Auf diese Weise soll vermieden werden, dass der Nutzer missbräuchlich für Newsletter-Abonnements angemeldet wird oder dass Fehler bei der Adresseingabe dazu führen, dass er keine Nachrichten erhält. Bestätigt er die Anmeldung, ist der „Double-Opt-In“ abgeschlossen und es liegt eine wirksame Einwilligung des Betroffenen vor.
Im Ergebnis stellte der TLfDI daher fest, dass durch das angewandte und auch zulässige „Double-Opt-In“-Verfahren eine wirksame Einwilligung des Betroffenen vorlag. Das Verfahren wurde vom TLfDI abgeschlossen.

Wer Newsletter verschicken möchte, ist gesetzlich dazu verpflichtet, den Empfänger vorher um Erlaubnis zu fragen § 4 Abs. 1 i. V. m. § 28 Abs. 3 Satz 1 BDSG. Hierfür ist das „Double-Opt-In“-Verfahren einzusetzen. Für die Einwilligung reicht der einfache Opt-In (Kunde erteilt eine Einwilligungserklärung durch Ankreuzen oder eine gesonderte Unterschrift) auf einer Webseite nicht aus; es wird ein Double-Opt-In benötigt. Wie schon die Bezeichnung vermuten lässt, setzt dieser die zweimalige Zustimmung des Kunden voraus. Nach dem ersten Opt-In erhält der Kunde eine kurze E-Mail mit der Bitte, seine Einwilligung per Klick auf einen Bestätigungslink end-

gültig zu bestätigen. Erst wenn er diesen Link geklickt hat, ist der Double-Opt-In abgeschlossen und der Kunde darf in den Verteiler für den Newsletter aufgenommen werden.

8.5 Datenabgleich bei kulturellen Veranstaltungen

Haben Sie schon einmal erlebt, dass Sie an der Einlasskontrolle zu einer kulturellen Veranstaltung nach Ihrem Namen gefragt wurden? Im Rahmen einer Beschwerde wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam, dass bei einem Veranstalter personenbezogene Daten bereits beim Kauf der Eintrittskarten erhoben wurden. Der Veranstalter rechtfertigte die Datenerhebung mit dem Service, Karten zu versenden, Rechnungen zuzustellen, Organisatorisches zu klären, Veranstaltungsabläufe zu besprechen, den individuellen Tischplan zu erstellen und bei Veranstaltungsabsage oder Verlegung in ein anderes Haus den Gast zu informieren. Gleichzeitig wurde der Versand einer Zeitschrift vom Veranstalter angeboten. Keineswegs wurde der Käufer beim Erwerb der Eintrittskarten auf eine Freiwilligkeit der Angabe seiner personenbezogenen Daten hingewiesen. Vielmehr betonte der Käufer, dass die Karten ohnehin verschenkt werden würden und ein späterer Rückschluss auf den Käufer ohnehin nicht möglich sei.
Grundsätzlich musste es dem Käufer möglich sein, Eintrittskarten für Veranstaltungen ohne Angabe seiner personenbezogenen Daten zu erwerben. Denn das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des Bundesdatenschutzgesetzes (BDSG) oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Eine gesetzliche Grundlage zur Erhebung der Käuferdaten lag nicht vor. Nicht jeder Käufer wünschte die Zusendung der Zeitschrift. Jedenfalls bei Barzahlung der Eintrittskarten war die Erhebung der Käuferdaten nicht erforderlich. Die Käufer der Veranstaltungstickets waren oftmals nicht die Besucher der Veranstaltung. Gerade zu Weihnachten oder zu Geburtstagen werden gern Eintrittskarten verschenkt. Auch ist es nicht unüblich, die Karten bei Krankheit oder Urlaub an Freunde/Bekannte weiter zu verschenken. Selbst wenn der Käufer einer Karte auch Besucher einer Veranstaltung war, war die Angabe des Namens der Besucher auch nicht beim Einlass erforder-

lich. Die Besucher hätten sich auch ohne Angabe ihres Namens und nur unter Angabe der Personenzahl eine gestellte Tischvariante aussuchen können. Gerade bei Beschenkten führte die Namensangabe nicht zum Ziel, sich einen Tisch, der für die gewünschte Personenzahl genügend Platz bietet, auszusuchen und konnte auch nicht mit einer internen Liste abgeglichen werden. Gleiches galt für die Besucher, welche die Eintrittskarten von Beschenkten bekommen hatten.
Eine Datenerhebung kam nur aufgrund der Einwilligung der Käufer in Betracht. Die Einwilligung der Käufer war grundsätzlich nur wirksam, wenn sie auf deren freie Entscheidung beruhte und, zumindest beim Verkauf vor Ort, schriftlich erfolgte, § 4a Abs. 1 BDSG. Wenn der Kartenverkauf schon an die Bedingung der Preisgabe von Käuferdaten geknüpft war, war diese Einwilligung unwirksam. Die Käufer waren vor der Angabe ihrer personenbezogenen Daten darauf hinzuweisen, dass die Angabe freiwillig erfolgte und für welche Zwecke diese erhoben wurden. Käufer, die sich für die Angabe ihrer Daten entschieden hatten, mussten mit einer weiteren Einwilligung dem Versand der Zeitschrift zustimmen, § 28 Abs. 3 BDSG, da es sich insoweit um Werbung im Sinne des BDSG handelte. Die Betroffenen waren ebenfalls über ihr Widerspruchsrecht zu unterrichten, § 28 Abs. 3a und 4 BDSG. Da die Käuferdaten grundsätzlich nur auf deren Anfrage gelöscht wurden, wurde der Veranstalter weiterhin aufgefordert, diese dann zu löschen, wenn sie nicht mehr erforderlich sind. Im Regelfall war dies nach dem Ende einer jeden Veranstaltung. Wurde dem Versand der Zeitschrift zugestimmt, waren die personenbezogenen Käuferdaten gemäß § 28 Abs. 4 BDSG spätestens dann zu löschen, wenn der Bewerbung widersprochen wurde.

Es bleibt zu beobachten, ob die Forderungen des TLfDI umgesetzt werden. Andernfalls wird der TLfDI eine Anordnung nach § 38 Abs. 5 BDSG treffen, die darauf abzielt, die verantwortliche Stelle zu zwingen, das geltende Datenschutzrecht einzuhalten.

Werden personenbezogene Daten ohne gesetzliche Grundlage erhoben, ist eine Einwilligung der Betroffenen erforderlich, § 4 Abs. 1 BDSG. Diese ist nur wirksam, wenn die Abgabe der Einwilligung nicht an den Abschluss des Kaufvertrags gebunden ist. Wird zusätzlich eine Werbung für eigene Produkte angeboten, ist eine weitere Zustimmung nach § 28 Abs. 3 BDSG erforderlich. Diese ist in

drucktechnisch deutlicher Gestaltung besonders von der Einwilligungserklärung hervorzuheben.

8.6 Lettershopverfahren – unerwünschte Werbung?

Werbung kann anregen, aufregen oder einfach nur stören. In engem Zusammenhang mit unerwünschter Werbung steht der Handel mit Adressen und anderen werberelevanten Daten. In diesem Berichtszeitraum wandte sich der Bevollmächtigte eines Energieversorgungsunternehmens mit folgender Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Im Sommer 2014 hatte ein Konkurrenz-Energieversorgungsunternehmen im Rahmen einer besonderen Marketingaktion mittels eines Werbeschreibens ausschließlich die Kunden des beschwerdeführenden Energieversorgungsunternehmens angeschrieben. Dieses Werbeschreiben richtete sich nur an die Bestandskunden des Energieunternehmens, Kunden anderer Anbieter erhielten kein solches Werbeanschreiben durch das Konkurrenzunternehmen. Grund der Werbeaktion war der Verlust einiger Kunden in der Vergangenheit. Mit diesem Werbeanschreiben versuchte man, diese Wechselkunden wieder zurückzugewinnen. Nach Aussage des Bevollmächtigten habe gerade die Ausgestaltung des Werbeanschreibens erkennen lassen, dass es sich um ein maßgeschneidertes Exklusiv-Angebot für Bestandskunden des Energieversorgungsunternehmens gehandelt hat.

Um die Zulässigkeit der Werbeaktion beurteilen zu können, wurde das Konkurrenz-Energieversorgungsunternehmen um Stellungnahme gebeten. Denn nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Nutzung von personenbezogenen Daten für Zwecke der Werbung nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Soweit es sich bei den angeschriebenen Kunden um ehemalige Kunden des Unternehmens gehandelt hat, waren nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG die personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war.

Darüber hinaus ist nach § 28 Abs. 3 BDSG die Verarbeitung oder Nutzung personenbezogener Daten für Werbezwecke grundsätzlich nur zulässig, soweit der Betroffene eingewilligt hat, § 28 Abs. 3 S. 1 BDSG. Es gibt aber einige Ausnahmen von diesem Grundsatz. Bei bestimmten personenbezogenen Daten – Name, Anschrift, Titel,

akademischer Grad, Geburtsjahr, Berufs-, Branchen- oder Geschäftsbezeichnung – (man spricht dabei auch von so genannten Listendaten), die das werbende Unternehmen von den Kunden selbst erhalten oder aus öffentlichen Branchen-, Adress- oder Telefonverzeichnissen entnommen hat, ist es auch ohne Einwilligung möglich, dass diese Daten für Zwecke der Werbung genutzt und weitergegeben werden, solange nicht widersprochen wurde oder die verantwortliche Stelle nicht aus sonstigen Gründen annehmen musste, dass schutzwürdige Interessen der Werbenutzung entgegengestanden haben.

Das Unternehmen teilte dem TLfDI mit, dass es sich bei der durchgeführten Werbeaktion nicht um ein vermeintliches Kundenrückgewinnungsprojekt gehandelt habe. Vielmehr wurde im Rahmen der Werbeaktivität Neukundenakquise im so genannten Lettershopverfahren nach § 28 Abs. 3 S. 5 BDSG betrieben. Bei einem Lettershopverfahren stellt das werbende Unternehmen dem Adresshändler und -inhaber, dem Lettershop, sein Werbematerial zur Verfügung. Der Adresshändler wählt nach bestimmten Kriterien Adresssätze aus. Diese werden dann mit der noch nicht adressierten Werbung des werbenden Unternehmens zusammengeführt und vom Adresshändler selbst versendet. Die Adressdaten werden folglich nicht an das eigentlich werbende Unternehmen „übermittelt“. Es findet kein Datenhandel statt. Das werbende Unternehmen erhält nur und erst dann Kenntnis von der Kundenadresse, wenn der Beworbene mit einer Bestellung reagiert.

Dieses Verfahren hat der Gesetzgeber in § 28 Abs. 5 BDSG für ausdrücklich zulässig erklärt. Einzige Voraussetzung ist, dass in einem solchen Anschreiben entsprechend auf die verantwortliche Stelle, also auf den Adresshändler, hingewiesen wird. Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere in Auftrag vornehmen lässt. Diesen Anforderungen, einen Hinweis auf die verantwortliche Stelle zu geben, kam hier der Lettershop, also der Adresshändler, als verantwortliche Stelle nach.

Der TLfDI konnte im Ergebnis feststellen, dass zum Zwecke der Werbeaktion keinerlei Daten von dem Konkurrenzunternehmen aus einem ehemaligen Kundendatenstamm verwendet wurden. Der TLfDI teilte daraufhin dem Bevollmächtigten mit, dass vorliegend kein

Verstoß gegen datenschutzrechtliche Bestimmungen vorgelegen hatte.

Bei einem Lettershopverfahren stellt das werbende Unternehmen dem Adresshändler, dem Lettershop, sein Werbematerial zur Verfügung. Letzterer wählt aus seinem Adressfundus nach den vereinbarten Kriterien Adressen aus, führt diese mit dem Werbematerial zusammen und organisiert den Versand. Nach § 28 Abs. 3 Satz 5 BDSG dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle, also der Adresshändler, eindeutig erkennbar ist.

8.7 Einladung zum falschen Klassentreffen in falscher Schule

Wenn Sie schon einmal eine Einladung zum Klassentreffen bekommen haben, ohne überhaupt in dieser Klasse gewesen zu sein, fragen Sie sich sicher, woher die Einladung kommt. Genau so ging es einem Beschwerdeführer. Er wunderte sich, warum er überhaupt zum Klassentreffen eingeladen wurde, obwohl er gar nicht in dieser Klasse gewesen und auch nicht in diese Schule gegangen war. Aber am meisten interessierte ihn die Frage, woher denn überhaupt seine personenbezogenen Daten gekommen waren und warum er mit dieser Klasse und dieser Schule in Verbindung gebracht wurde.
In diesem Fall hatte der Betroffene gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) das unabdingbare Recht, selbst beim Absender ein Auskunftsersuchen zu stellen. Damit konnte er in Erfahrung bringen, ob und welche personenbezogenen Daten über ihn gespeichert waren, aus welchen Quellen diese Daten stammten und zu welchem Verwendungszweck sie bei wem gespeichert wurden. Der Betroffene wollte sich zunächst selbst an die Ersteller der Einladung als verantwortliche Stelle wenden. Dabei wurde ihm geraten, eine Frist zur Antwort zu setzen. Er wollte sich wieder beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) melden, sollte er bis zum Ablauf dieser Frist keine Antwort erhalten haben.
Da der TLfDI keine Rückmeldung vom Beschwerdeführer erhalten hatte, scheint dieser mit seinem Auskunftsersuchen erfolgreich gewesen zu sein.

Den Betroffenen steht gemäß § 34 BDSG ein Auskunftsrecht gegenüber der verantwortlichen Stelle zu. Wird ein Auskunftsbegehren ignoriert, kann sich der Betroffene an den TLfDI als zuständige Aufsichtsbehörde wenden. Unterbleibt eine Antwort auf das Auskunftsersuchen, kann der verantwortlichen Stelle die Auskunftserteilung gemäß § 38 Abs. 5 BDSG angeordnet werden. Außerdem kann gegen den Auskunftsverpflichteten ein Bußgeldverfahren nach § 43 Abs. 1 Nr. 8a BDSG eingeleitet werden.

8.8 Unerlaubte Telefonwerbung

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines Bürgers. Nach seinen Angaben erhielt er von einer Organisation in Thüringen unaufgefordert aufdringliche Telefonwerbeanrufe. Die Telefonnummer, von welcher die aufdringliche Telefonwerbung erfolgte, teilte der Bürger dem TLfDI mit.
Der TLfDI hat sich daraufhin an die Bundesnetzagentur gewandt und um Auskunft über den Inhaber dieser Telefonnummer gebeten. Die Bundesnetzagentur teilte dem TLfDI mit, dass Ortsnetzrufnummern in einem zweistufigen Verfahren von der Bundesnetzagentur in 1000er Rufnummernblöcken an Anbieter von Telekommunikationsdiensten und von diesen an Endkunden zugeteilt würden. Im Anschluss daran hat der TLfDI den von der Bundesnetzagentur benannten Anbieter von Telekommunikationsdiensten um Auskunft über den Inhaber der vorgenannten Telefonnummer gebeten. Diese Mitteilung liegt dem TLfDI bisher noch nicht vor. Soweit der TLfDI über den Inhaber der Telefonnummer Kenntnis hat, wird er diesen zur Auskunft zum Sachverhalt gemäß § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) auffordern.
Allgemein lässt sich jedoch sagen, dass immer wieder Telefonwerbeaktionen von Unternehmen Anlass zur Beschwerde von Betroffenen bieten. Grund hierfür ist oftmals die unzulässige Verwendung personenbezogener Daten zu Zwecken der Telefonwerbung entgegen klarer gesetzlicher Vorgaben. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BSGD oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. § 28 Abs. 3 BDSG bildet die datenschutzrechtliche Grundlage für

die Erhebung, Übermittlung und Nutzung personenbezogener Daten zu Zwecken der Werbung und knüpft diese an eine Vielzahl an Bedingungen. Auch hier gilt grundsätzlich, dass das Durchführen von Telefon-Direkt-Marketing-Aktionen die Einwilligungserklärung der Betroffenen voraussetzt, § 28 Abs. 3 Satz 1 BDSG. Diese Einwilligungserklärungen sind dann nur unter bestimmten Bedingungen wirksam, § 4a BDSG: Zunächst muss die Einwilligungserklärung von den Betroffenen ausdrücklich abgegeben worden sein. Weiterhin sind die Betroffenen in der Einwilligungserklärung darüber zu informieren, zu welchem Zweck ihre personenbezogenen Daten erhoben und verarbeitet werden. Auch muss die Einwilligungserklärung darüber Auskunft geben, an wen die personenbezogenen Daten weitergeleitet werden sollen. Die Abgabe einer Einwilligungserklärung darf nicht an Bedingungen geknüpft werden und sie muss Auskunft darüber geben, welches Kontaktmedium genutzt werden soll. Schließlich sind die Einwilligungserklärungen durch das die Daten erhebende Unternehmen in geeigneter Form aufzubewahren, sodass in Streitfällen gegenüber dem Betroffenen der Nachweis erbracht werden kann, dass er vormals eine Einwilligungserklärung abgegeben hat. Auch entschied der Bundesgerichtshof (BGH) mit dem Urteil "Telefonaktion II" vom 10. Februar 2011 (Az.: I ZR 164/09), dass Unternehmen grundsätzlich nur dann Werbeanrufe bei Privatpersonen tätigen dürfen, wenn diese zuvor eine Einwilligungserklärung abgegeben haben.

Nach § 28 Abs. 3 Satz 2 kann eine Verarbeitung oder Nutzung von personenbezogenen Daten zu werblichen Zwecken nämlich nur dann ohne Einwilligung der Betroffenen erfolgen, wenn Angaben über Personen, die einer Gruppe angehören, in Listen zusammengefasst verwendet werden. § 28 Abs. 3 Satz 2 BDSG legt verbindlich fest, welche Daten in solchen Fällen verarbeitet oder genutzt werden dürfen. Die verantwortliche Stelle hat also keine Wahl, sie muss sich auf die dort aufgeführten Daten beschränken. Dabei handelt es sich um die Angabe zur Zugehörigkeit des Betroffenen zur jeweiligen Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, zum Namen, Titel, akademischen Grad, zu Anschrift und Geburtsjahr. Die Telefonnummer zählt gerade nicht zu diesen „Listendaten“.

Über den Ausgang des Verfahrens wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Telefonwerbung ist nach § 28 Abs. 3 Satz 1 BDSG nur dann erlaubt, wenn die Betroffenen vorher ausdrücklich der telefonischen Werbung des entsprechenden Unternehmens zugestimmt haben. In allen anderen Fällen handelt es sich um unerlaubte Telefonwerbung. In solchen Fällen sollten sich Betroffene nicht nur an den TLfDI wenden, sondern ebenfalls an die Bundesnetzagentur.

8.9 Dubioses Verkaufsangebot: 800 Euro für eine Million E-Mail-Adressen

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde darüber informiert, dass ein Unternehmen E-Mails versandt hatte, in denen der Verkauf von Emailadressen angeboten wurde. Der Anbieter der E-Mail-Adressen versuchte damit, seinen Bestand von ca. über einer Million deutscher E-Mail-Adressen gewinnbringend zu veräußern, wobei der Preis für eine Million E-Mail-Adressen 800 Euro betragen sollte.
Der TLfDI gab daraufhin die Eingabe des Bürgers an die Staatsanwaltschaft zum Zwecke der Strafverfolgung einer Straftat nach § 43 Abs. 2 i. V. m. § 44 Abs. 1 Bundesdatenschutzgesetz (BDSG) ab. Denn wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet (= an einen Dritten weitergibt, § 3 Abs. 4 BDSG) und dies vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, erfüllt einen Straftatbestand nach § 43 Abs. 2 i. V. m. § 44 Abs. 1 BDSG. Dies kann eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe nach sich ziehen.

In der Folge veröffentlichte das Landeskriminalamt (LKA) Niedersachsen auf seiner Homepage unter „Aktuelles“ (http://www.polizei-prävention.de) einen Artikel mit folgendem Inhalt: „Leider ist das Anbieten solcher Emailadressen noch nicht strafrechtlich sanktioniert, d. h. das Anbieten solcher Adressen ist straffrei. Es ist allerdings anzunehmen, dass diese Daten mit hoher Wahrscheinlichkeit nicht aus legalen Quellen, sondern aus illegalen Datenabgriffen im Internet stammten. Aufgrund der (noch) fehlenden Strafbarkeit der Hehlerei von Daten, gibt es für die Polizei leider keine strafprozessualen Ansätze. In der Zentralstelle Cyber-

crime des LKA Niedersachsen wurden unabhängig davon aber Recherchen durchgeführt, um weitergehende Erkenntnisse zu gewinnen."
Darüber hinaus teilte das LKA Niedersachsen mit, dass auch der Datenschutzbeauftragte des Landes Niedersachsen über das Vorgehen informiert wurde. Nach Einschätzung des Datenschutzbeauftragten des Landes Niedersachsen bestand keine Zuständigkeit der Datenschutzbeauftragten in Deutschland, weil es keinerlei Hinweise auf einen Aufenthalt des Verkäufers in Deutschland gab
Nach § 1 Abs. 5 BDSG findet das Bundesdatenschutzgesetz keine Anwendung, sofern eine in einem anderen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Da hier keine Hinweise auf Aktivitäten der verantwortlichen Stelle oder einer Niederlassung in Deutschland vorlagen, war das BDSG im Sinne des § 1 Abs. 5 Satz 1 letzter Halbsatz BDSG nicht anwendbar. Das Ergebnis des Ermittlungsverfahrens liegt dem TLfDI noch nicht vor.

Bei verantwortlichen Stellen, die innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums belegen sind, scheidet eine Anwendung des BDSG grundsätzlich aus, vergleiche § 1 Abs. 5 Satz 1 BDSG. Das BDSG stellt nicht auf den Sitz des Unternehmens, sondern auf den Ort der aktiven Niederlassung (Niederlassungsprinzip) ab. Kunden und andere Betroffene, die mit der deutschen Niederlassung eines ausländischen Unternehmens aus dem EU-/EWR-Raum zu tun haben, werden infolgedessen nicht mit dem ausländischen Recht konfrontiert, sondern haben die gleichen Rechte aus dem BDSG wie gegenüber deutschen Stellen.

8.10 Absprung mit Daten – Werbung in der Versicherungsbranche

Im Sommer 2015 ist dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein besonders schwerer Fall einer „Datenmitnahme" durch einen Versicherungsvertreter beim Wechsel zu einem anderen Versicherungsberatungsunternehmen bekannt geworden. Der Beschwerdeführer hatte sich

zunächst „nur“ über Werbeschreiben seines Versicherungsberaters beklagt. Allerdings sei dieser im Namen eines anderen Versicherungsunternehmens aufgetreten. Im Laufe der Beschwerdebearbeitung verhärtete sich der Verdacht einer unberechtigten Datenerhebung und -verarbeitung des Versicherungsberaters.
Daraufhin wurde zunächst ein Bußgeldverfahren gemäß § 43 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) eingeleitet. Nun bestätigte sich die Vermutung des TLfDI recht schnell. Der Versicherungsberater übernahm schon im Jahr 2008 eine Bezirksagentur einer Versicherung. Er erhielt einen zu betreuenden Kundenstamm von ca. 600 Kunden. Bereits im Sommer 2013 nahm er eine Selektion der Kundendaten aus dem Online-Vertriebsportal der Versicherung zu angeblichen Vertriebsaktionen vor. Nachdem der Versicherungsberater das Arbeitsverhältnis kündigte, wurde er mit sofortiger Wirkung von der Tätigkeit für das Unternehmen und dessen Kooperationspartner entbunden. Von nun an hat der Versicherungsvertreter sein Unwesen getrieben. Der Aufforderung, sämtliche Unternehmensunterlagen zurückzugeben, kam er auch nach mehrmaliger Erinnerung nicht nach. Der Zugang zu dem Online-Vertriebsportal der Versicherung war für ihn gesperrt. Unterdessen schien der Versicherungsberater zwischenzeitlich für ein anderes Versicherungsunternehmen tätig geworden zu sein und dafür die Kundendaten aus der o. g. Selektion aus seinem vorherigen Arbeitsverhältnis verwendet zu haben. Dies war insbesondere dadurch aufgefallen, dass überdurchschnittlich viele Kunden ihre Verträge bei dem alten Versicherungsunternehmen kündigten. Gleichzeitig gingen mehrere Beschwerden ein, dass Kundenverträge in ihrem Namen gekündigt wurden, obwohl dies von den Kunden nicht beabsichtigt war und diese die Kündigungsschreiben nicht selbst unterschrieben hatten. Weiterhin beschwerten sich die Kunden über Werbung des neuen Versicherungsunternehmens durch den Versicherungsberater.
Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Eine Einwilligung des Beschwerdeführers zur Erhebung seiner Daten lag nicht vor. Auch eine gesetzliche Ermächtigung war hier nicht gegeben. Der Versicherungsberater war weder nach § 28 Abs. 1 Nr. 1 BDSG dazu ermächtigt, die Kundendaten des Versicherungsunternehmens zu erheben noch diese zu verarbeiten.

Er hatte die Kundendaten der Versicherung nicht für den Zweck der Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit den Kunden dieses (neuen) Versicherungsunternehmens erhoben. Auch war eine Erhebung dieser Daten nach § 28 Abs. 1 Nr. 2 BDSG nicht erforderlich. Jedenfalls überwogen die schutzwürdigen Interessen der Kunden des alten Versicherungsunternehmens an dem Ausschluss der Datenerhebung das Interesse des Versicherungsberaters an diesen Daten. Er hatte die Kundendaten vielmehr erhoben, um diese später für ein anderes Unternehmen zu Zwecken der Werbung zu verarbeiten. Eine Verwendung der erhobenen Daten zu diesem anderen Zweck nach § 28 Abs. 2 Nr. 1 BDSG kam hier ebenfalls nicht in Betracht, da die schutzwürdigen Interessen der Kunden des alten Versicherungsunternehmens an einem Ausschluss der Übermittlung ihrer personenbezogenen Daten die Interessen des Versicherungsberaters überwogen. Ebenfalls waren die Kundendaten des alten Versicherungsunternehmens nicht allgemein zugänglich. Eine Verarbeitung und Nutzung der Daten aus der Kundenübersicht zum Zwecke der Werbung nach § 28 Abs. 3 BDSG war ebenfalls unzulässig, da schon die Erhebung der Kundendaten unzulässig erfolgte. Da hier keine Erlaubnisnorm zur Erhebung der Kundendaten der alten Versicherung vorlag, war die Datenerhebung nach § 4 Abs. 1 BDSG insgesamt unzulässig. Eine weitere Verarbeitung oder Nutzung dieser Daten, die über Werbezwecke hinausging, war danach ebenfalls unzulässig.
Der Versicherungsberater hatte die Kundenselektion bei der Versicherung im Sommer 2013 vorsätzlich, mit der Absicht sich selbst zu bereichern und dem Versicherungsunternehmen Schaden zuzufügen, vorgenommen. Da hier allem Anschein nach eine Straftat mit Schädigungsabsicht bzw. Bereicherungsabsicht vorlag, hatte der TLfDI nach § 44 Abs. 2 BDSG als Antragsberechtigter einen Strafantrag gestellt und das Bußgeldverfahren insoweit an die Staatsanwaltschaft abgegeben. Zeitgleich wurde der Versicherungsberater aufgefordert, die unzulässig erhobenen Kundendaten der alten Versicherung gemäß § 3 Abs. 4 Nr. 5 BDSG zu löschen. Für den Fall, dass er dieser Forderung nicht nachkommt, wurde der Erlass einer Anordnung nach § 38 Abs. 5 BDSG angedroht.

Neben dem Strafantragsrecht gemäß § 44 Abs. 2 BDSG hat der TLfDI im Verwaltungsverfahren weitere Möglichkeiten, die Wiederherstellung datenschutzkonformer Zustände zu bewirken. Dazu

gehören die Anordnung und die Festsetzung eines Zwangsgeldes nach § 38 Abs. 5 BDSG. Ungeachtet dessen hat der TLfDI die Möglichkeit, bei Verstößen nach § 43 BDSG ein Ordnungswidrigkeitenverfahren einzuleiten. Je nach Schwere des Verstoßes sind Geldbußen von bis zu 300.000 Euro möglich.

8.11 Versicherungsdaten abgeschleppt

Eine Beschwerde von einem Versicherten lenkte die Aufmerksamkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum auf einen kuriosen Fall einer „Datenmitnahme“ eines Versicherungsmaklers. Der Versicherte monierte, dass sein Versicherungsmakler zukünftig nicht mehr mit dem bisherigen Versicherungsbüro A zusammenarbeite. Dieser bat daher alle Kunden des Versicherungsbüros A, mittels einer schriftlichen Einwilligungserklärung sämtliche Versicherungspolicen in seine Betreuung umzustellen. Unabhängig davon konnte der TLfDI, wie in dem Beitrag Nummer 2.41 dargestellt, aufklären, dass der Versicherungsmakler von dem Versicherungsbüro A eine Vielzahl von Datensätzen in ausgedruckter sowie in digitaler Form mitnahm. So unter anderem alle Kunden- und Vertragsdaten. Der Versicherte willigte zwar zunächst in die Betreuungsumstellung ein, widerrief aber nach zwei Wochen seine Einwilligung zur Umstellung. Grund dafür war, dass sein Versicherungsmakler nun, entgegen seinen Angaben als unabhängiger Versicherungsmakler tätig werden zu wollen, mit dem Versicherungsbüro B zusammenarbeitete. Die Umstellung der Versicherungspolicen bei den jeweiligen Versicherungsunternehmen überschnitt sich dann mit dem Widerruf des Versicherten. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des Bundesdatenschutzgesetzes (BDSG) oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). In diesem Fall fand die Übertragung der bestehenden Versicherungspolicen zunächst aufgrund der Einwilligung des Versicherten statt. Diese ist jedoch dann mit dem Widerruf weggefallen. Somit lag eine aktuell gültige Einwilligung nicht mehr vor. Mit dem Erhalt des Widerrufs von dem Versicherten hatte der Versicherungsmakler ohne Aufforderung des TLfDI sofort begonnen, die Umstellung der Versiche-

rungspolicen über das Versicherungsbüro B rückgängig zu machen. So weit, so gut.
Neun Monate nach der Rückabwicklung erinnerte der Versicherungsmakler das Versicherungsunternehmen erneut an die Bestandsübertragung der Versicherungspolicen des Versicherten vom Versicherungsbüro A an das Versicherungsbüro B. Dabei legte der Versicherungsmakler dem Versicherungsunternehmen die damals unterzeichnete schriftliche Einwilligungserklärung zur Betreuungsumstellung des Versicherers vor. Ohne Prüfung des vorgelegten Vertrages stellte das Versicherungsunternehmen die Versicherungspolicen erneut um und benachrichtigte den Versicherten darüber.
Erst auf Verlangen des TLfDI überprüfte das Versicherungsunternehmen die erneut übersandte schriftliche Einwilligung des Versicherten auf Aktualität. Dabei stellte das Versicherungsunternehmen fest, dass die Einwilligungserklärung des Versicherten das Datum von vor neun Monaten aufwies.
Es erfolgte eine Rückabwicklung des Vertrages mit Versicherungsbüro B auf das Versicherungsbüro A. Da hinsichtlich der „Datenmitnahme“ die Verwirklichung eines Ordnungswidrigkeitentatbestands im Raum steht und dieser darüber hinaus mit Bereicherungsabsicht erfüllt worden sein könnte, hat der TLfDI von seinem Recht, einen Strafantrag zu stellen, Gebrauch gemacht und die Staatsanwaltschaft über die „Datenmitnahme“ durch den Versicherungsmakler in 1.300 Fällen informiert.

Nach 4 Abs. 1 BDSG ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des Bundesdatenschutzgesetztes (BDSG) oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Soweit die Datenerhebung und -verarbeitung aufgrund einer Einwilligungserklärung stattfindet, muss die Einwilligung des Betroffenen auch aktuell und gültig sein. Strafbares Handeln im Sinne des BDSG liegt vor, wenn zu einer Ordnungswidrigkeit gemäß § 43 Abs. 2 BDSG noch weitere Merkmale (§ 44 BDSG) hinzukommen, nämlich die dort genannten Merkmale des Handelns gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht.

Stethoskop mit Gesundheitskarte auf Geldscheinen – © Zerbor / Fotolia.com

9 Gesundheit

9.1 Auslagerung von Krankenhausakten zulässig?

Ein Klinikum aus Thüringen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Beratung zu folgender Frage:
In dem Unternehmen werde derzeit die Möglichkeit geprüft, die Archivierung der Patientenakten durch einen externen Dienstleister erbringen zu lassen. Mittelfristig bestehe das Ziel, keinerlei Papierakten mehr zu archivieren, sondern die Langzeitarchivierung ausschließlich digital durchzuführen. Das Krankenhaus bat um Mitteilung, worauf bei der Auslagerung von Patientenakten geachtet werden müsse und wollte wissen, ob es hierzu eine Orientierungshilfe gibt. Der TLfDI teilte dem Krankenhaus mit, dass, wenn in einem Krankenhaus Patientenakten ausgelagert würden, dies nur unter den Voraussetzungen des § 27b Thüringer Krankenhausgesetz (ThürKHG) möglich sei. Danach sind Patientendaten grundsätzlich im Krankenhaus zu verarbeiten. Eine Verarbeitung und Nutzung durch eine andere Stelle im Auftrag ist nur zulässig, wenn sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der

automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können. Dabei muss die Einhaltung der Datenschutzbestimmungen des ThürKHG sowie eine den Voraussetzungen des § 203 Strafgesetzbuch entsprechende Schweigepflicht beim Auftragnehmer sichergestellt sein. Der Auftraggeber hat darüber hinaus der Aufsichtsbehörde nach § 32 Abs. 2 ThürKHG rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich anzuzeigen.
Diese Voraussetzungen müssen gegenüber der Aufsichtsbehörde nachgewiesen werden. Die Aufsichtsbehörde nach § 32 Abs. 2 Thüringer Krankenhausgesetz (ThürKHG) ist das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie. Im Vertrag über die Auftragsdatenverarbeitung ist sicherzustellen, dass vom Auftraggeber oder von dessen Datenschutzkontrollbehörde veranlasste Kontrollen vom Auftragnehmer jederzeit zu ermöglichen sind. Weiterhin sind im Vertrag die technischen und organisatorischen Maßnahmen festzulegen, die erforderlich sind, um eine Kenntnisnahme Unbefugter zu verhindern und die Authentizität und Integrität der Dokumente zu gewährleisten. Der Dienstleister ist so zu wählen, dass dieser die für das Krankenhaus erforderlichen technischen und organisatorischen Anforderungen gewährleisten kann. Die konkret zu treffenden technischen und organisatorischen Maßnahmen hängen immer von den Umständen des Einzelfalles ab. Eine Orientierungshilfe zu dem Thema existiert derzeit leider nicht, weswegen der TLfDI an der Erstellung einer solchen Orientierungshilfe arbeitet (siehe Nummer 3.1). Der TLfDI stellte klar, dass er zur Beantwortung von konkreten Fragen gerne zur Verfügung steht. Das Krankenhaus hat dieses Angebot bislang nicht aufgegriffen.

Anders als bei praktizierenden Ärzten gibt es in Thüringen für Krankenhäuser eine Bestimmung, nach der Patientendaten im Rahmen der Auftragsdatenverarbeitung ausgelagert werden können. Die dazu erforderlichen Voraussetzungen sind in § 27b ThürKHG abschließend aufgeführt.

9.2 Umgang mit Patientenakten bei Praxisübergabe

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Eingabe einer Bürgerin, die

sich über den Umgang mit ihren Patientenakten bei einem niedergelassenen Arzt beschwerte. Nach Schilderungen der Bürgerin war sie als Patientin bei einer bestimmten Ärztin jahrzehntelang in Behandlung. Die Praxis war dann an einen neuen Arzt übergeben worden. Damit sei auch ihre Patientenakte an den Praxisnachfolger übermittelt worden. Die Beschwerdeführerin war deshalb der Meinung, dass der neue Arzt mit dem erfolgten Praxiswechsel bei ihr eine Einwilligung zur weiteren Aufbewahrung ihrer Patientenakte in der Praxis hätte einholen müssen. Die Beschwerdeführerin kritisierte darüber hinaus, dass die Patientenakte ohne ihre Einwilligung eingescannt, also digitalisiert worden sein soll. Der TLfDI teilte der Beschwerdeführerin mit, dass er sich bereits im letzten Tätigkeitsbereich für den nicht-öffentlichen Bereich zu den angesprochenen Fragen geäußert hatte. Danach handelt es sich bei Patientenakten nach § 3 Abs. 9 des Bundesdatenschutzgesetzes (BDSG) um besondere Arten von personenbezogenen Daten, da diese Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig. Grundsätzlich unterliegen die Patientendaten nicht dem Zugriff des neuen Inhabers. Diese werden nur im Falle der Einwilligung des Patienten für die neue Praxis aktiviert. Beim Praxisverkauf oder bei der Praxisübernahme ist zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten hat. Gemäß § 203 Abs. 1 Satz 1 Strafgesetzbuch wird derjenige mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, der unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis offenbart, welches ihm als Arzt anvertraut wurde. Der Verkauf einer Praxis oder die Insolvenz stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten muss es daher eine Einwilligungserklärung aller Patienten geben. Diese kann im Rahmen der laufenden Behandlung mündlich erfolgen, alle anderen Patienten müssen schriftlich befragt werden. Bei der Praxisübernahme wird daher oft auf das so genannte Zwei-Schränke-Modell zurückgegriffen. Dabei werden die übernommenen Patientenakten zunächst separat im ersten Schrank aufbewahrt. Sobald das Einverständnis erteilt worden ist, werden die Akten dann im laufenden System der übernehmenden Praxis eingefügt (zweiter Schrank). Aus der von der Beschwerdeführerin vorgebrachten Sachverhaltsdarstel-

lung konnte der TLfDI entnehmen, dass diese sich vom Praxisnachfolger nach ihren Angaben dort zweimal ein Rezept ausstellen ließ. Selbst wenn hierbei kein direkter Kontakt zwischen Arzt und Patient bestanden hatte, war der Arzt jedoch gehalten, die Indikationen für die erneute Verschreibung zu überprüfen. In diesem Fall durfte der „neue“ Arzt zunächst davon ausgehen, dass die Beschwerdeführerin dort weiterbehandelt werden wollte. Der Bundesgerichtshof führte in einem Urteil vom 11. Dezember 1991 - Az.: VIII ZR 4/91, Randnummer 45 hierzu aus, dass ein ausdrückliches Einverständnis dann nicht nötig sei, wenn der Patient sich in die Sprechstunde und Behandlung des neuen Arztes begebe, da er damit konkludent, also durch schlüssiges Verhalten, sein Einverständnis erkläre.
Was die Aufbewahrung von Patientendaten anbelangt, sind nach den bestehenden gesetzlichen Regelungen alle Patientenunterlagen nach Ablauf der jeweils geltenden Aufbewahrungsfristen datenschutzgerecht zu entsorgen. Es besteht nicht nur eine Pflicht des Arztes zur datenschutzgerechten Vernichtung von Patientenunterlagen. Vielmehr besteht grundsätzlich auch ein Recht des Patienten auf Löschung, also auf Unkenntlichmachung seiner Daten. Aus datenschutzrechtlicher Sicht ist es daher grundsätzlich notwendig, dass Daten nach Ablauf der jeweils geltenden Aufbewahrungsfristen gelöscht werden. Der Beschwerdeführerin wurde schließlich mitgeteilt, dass ein Verstoß des Arztes nach der Praxisübernahme im Umgang mit ihrer Patientenakte nicht festzustellen war. Ihr wurde angeboten, sich erneut an den TLfDI zu wenden, falls sich aus ihrer Sicht der Sachverhalt im Umgang mit ihren Patientenakten anders dargestellt hätte. Dies ist jedoch nicht erfolgt.

Die Nutzung von Patientendaten durch einen Arzt bei der Praxisnachfolge ist grundsätzlich nur mit Einwilligung des einzelnen Patienten zulässig. Es kann aber nach der Rechtsprechung des Bundesgerichtshofs eine Zustimmung daraus folgen, dass sich ein Patient in der Praxis weiter behandeln lässt. Auch das Ausstellen von Rezepten kann das Kriterium einer ärztlichen Behandlung erfüllen.

9.3 Übergabe einer Arztpraxis: Zwei-Schränke-Modell

Vielleicht kommt Ihnen der nachfolgende Sachverhalt auch bekannt vor: Seit Jahren sind Sie Patient des Arztes Ihres Vertrauens, der nun aber leider in den verdienten Ruhestand geht. Plötzlich müssen Sie

wieder zu einer Behandlung, wobei Sie feststellen, dass Sie nun ein unbekannter Nachfolger behandelt. Allein dieser Umstand ist für Sie, nachdem Sie endlich den Arzt des Vertrauens gefunden hatten, schon nicht einfach. Doch was ist eigentlich mit den Patientenunterlagen des Vorgängers passiert?

Aufgrund zunehmender Anfragen der Kammermitglieder an die Landesärztekammer zu Musterformulierungen von Patienteneinwilligungen wird seitens der Landesärztekammer beabsichtigt, ein entsprechendes Muster zu entwickeln und es den Ärzten zur Verfügung zu stellen. Um sicherzugehen, dass die Formulierungen den datenschutzrechtlichen Anforderungen entsprechen, wandte sich die Landesärztekammer mit der Bitte um Unterstützung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Bei Patientenakten handelt es sich nach § 3 Abs. 9 des Bundesdatenschutzgesetzes (BDSG) um besondere Arten von personenbezogenen Daten, da sie Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig. Beim Praxisverkauf oder bei der Praxisübernahme ist zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten der übernommenen Praxis hat. Gemäß § 203 Abs. 1 Satz 1 Strafgesetzbuch (StGB) wird derjenige mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, der unbefugt ein fremdes Geheimnis offenbart, welches ihm als Arzt anvertraut wurde. Der Verkauf oder die Übernahme einer Praxis stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten durch den neuen Arzt müssen daher jeweils für die einzelne Patientenakten Einwilligungserklärungen eingeholt werden. Diese können im Rahmen der laufenden Behandlung schriftlich erfolgen. Bei einer Praxisübernahme wird daher oft auf das sogenannte Zwei-Schränke-Modell zurückgegriffen. Dabei werden die übernommenen Patientenakten zunächst separat im ersten Schrank aufbewahrt. Sobald die Einwilligung der Patienten vorliegt, werden die Akten dann im laufenden System und somit im zweiten Schrank der übernehmenden Praxis eingefügt. Diese Bewertung hat der TLfDI bereits in seinem 1. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich unter der Nummer 3.33 (bis zur Bahre:

Patientenakten am Ende) vorgenommen. An dieser Bewertung hat sich auch in diesem Berichtszeitraum nichts geändert.

Die Landesärztekammer unterbreitete dem TLfDI nachfolgende Musterformulierung:
„Ich bin heute zur ärztlichen Behandlung bei (Praxisnachfolger) in dessen Sprechstunde erschienen. Mir ist bekannt, dass (Praxisnachfolger) zum (Datum der Praxisübergabe) die Praxis von (Praxisübergeber) übernommen hat. Ich willige ein, dass (Praxisnachfolger) zum Zwecke der medizinischen Behandlung Einsicht in meine bisher durch den (Praxisübergeber) geführte Patientenakte nehmen, alle vorhandenen medizinischen und sonstigen personenbezogenen Daten übernehmen und verwenden darf."

Diese vorgeschlagene Formulierung wurde seitens des TLfDI als sehr gelungen empfunden und nur noch dahingehend ergänzt, dass der Patient auf die Folge der Nichterteilung einer Einwilligung hinzuweisen ist.

„Ich wurde außerdem darüber belehrt, dass ich, sofern ich diese Einwilligung nicht erteile, behandelt werden muss, ohne dass (Praxisnachfolger) von meiner Patientenakte Kenntnis nehmen kann. Meine Patientenakte wird bis zum Ablauf der Aufbewahrungsfristen von (Praxisnachfolger) verwahrt, ohne dass dieser Einsicht nimmt, und sodann vernichtet."

Bei entsprechender Einwilligung durch den Patienten wird damit die Altpatientenakte Teil der neuen Patientenakte.
Schließlich hat der TLfDI die Landesärztekammer noch darauf hingewiesen, dass bei einer Weitergabe von personenbezogenen Daten an Dritte es auch hier einer Übermittlungsbefugnis in Form einer Erlaubnisnorm oder einer Einwilligung, neben einer ohnehin zu erteilenden Schweigepflichtentbindung, bedarf.

Die Verpflichtung zur ärztlichen Schweigepflicht besteht auch bei Übergabe und Verkauf einer Arztpraxis an einen anderen Arzt. Für die Übernahme der Patientenakten durch einen anderen Arzt bedarf es daher entsprechender Einwilligungserklärungen der Patienten zur Weitergabe ihrer Gesundheitsdaten. Bei entsprechender Einwilligung wird damit die Altpatientenakte Teil der neuen Patientenakte. Für

eine Praxisübernahme empfiehlt der TLfDI, auf das so genannte Zwei-Schränke-Modell zurückzugreifen.

9.4 Kränkelnde Studie – Datenschutz bei klinischen Studien

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Anfrage eines international tätigen Auftragsforschungsinstituts für klinische Studien. Das Unternehmen beabsichtigte, den Einsatz von bestimmten Medikamenten bei bestimmten Krankheitsbildern unter Alltagsbedingungen zu ermitteln. Dabei sollte eine Vielzahl an medizinischen und personenbezogenen Daten der Studienteilnehmer erhoben und verarbeitet werden. Das Unternehmen wandte sich mit seinem Anliegen an alle Aufsichtsbehörden. Die federführende Prüfung übernahm das Bundesland, in dem der deutsche Sitz des Unternehmens lag. Die dortige Aufsichtsbehörde koordinierte die Abstimmung über das Verfahren.
Die für die Studie zuständige Ethikkommission hatte in einem bedingt positiven Votum zu der Studie gefordert, eine ausreichende Pseudonymisierung der erhobenen Daten vorzunehmen. Ob diese Voraussetzungen vorlagen, wurde von der federführend zuständigen Aufsichtsbehörde geprüft. Sie äußerte wesentliche datenschutzrechtliche Bedenken im Hinblick auf die praktische Durchführung der Studie. Die vom Forschungsinstitut eingerichtete Datentreuhänderschaft ermöglichte keine ausreichende Sicherstellung der Pseudonymisierung von Teilnehmerdaten. Die wirtschaftliche Unabhängigkeit sowie dessen räumliche, organisatorische und personelle Trennung vom beauftragenden Unternehmen waren nicht erkennbar. Es war davon auszugehen, dass weder die zum Einsatz kommende Patienteninformation mit dem dargestellten Studienablauf noch die Einwilligungserklärung in der geprüften Form dem tatsächlichen Verfahren entsprachen. Die erteilte Einwilligung wäre damit unwirksam und der Prüfungsarzt setzte sich dem Risiko eines Verstoßes gegen die ärztliche Schweigepflicht aus, sofern er an der Studie teilnahm.
Da diese datenschutzrechtliche Einschätzung vom TLfDI geteilt wurde, informierte er die Landesärztekammer Thüringen über die mit der Studie bestehenden datenschutzrechtlichen Probleme für den Fall, dass das Forschungsunternehmen beabsichtigte, seine Studie auch in Thüringen durchzuführen. Die Landesärztekammer wurde gebeten, diese rechtliche Einschätzung zu berücksichtigen und an

ihre Ethikkommission weiterzuleiten, sollte das Forschungsunternehmen eine Bewertung der geplanten Studie beantragen.

Bei bundesweiten klinischen Studien übernimmt in der Regel die Aufsichtsbehörde des Bundeslands, in dem das Forschungsinstitut seinen Sitz hat, die Federführung bei der datenschutzrechtlichen Prüfung. Eine hinreichende Pseudonymisierung der personenbezogenen Daten ist nur gegeben, wenn ein Datentreuhänder wirtschaftlich, räumlich, organisatorisch und personell hinreichend unabhängig von der verantwortlichen Stelle (auftraggebendes Unternehmen) ist.

9.5 Rezeptbestellung via Messenger? – Nein!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum ein Bild von einem Werbeflyer, der darüber informierte, das ab sofort in einer Mühlhäuser Apotheke Arzneimittel mittels eines Nachrichtendienstes vorbestellt werden können. Dafür ist es notwendig, ein Foto der Medikamentenverpackung oder gar des Rezeptes zu senden. Vor allem bei Rezepten handelt es sich um Gesundheitsdaten und damit um besonders schützenswerte, besondere Arten von personenbezogenen Daten i. S. v. § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG). Weiterhin wird bei der Medikamentenbestellung eine Telefonnummer als personenbezogenes Datum an den Dienst übermittelt. Hierzu gibt es gleich mehrere Bedenken:
Die Server werden in den USA betrieben. Die Datenkanäle laufen auf jeden Fall dorthin. Angeblich werden Nachrichten bei diesem Dienst zwar Ende-zu-Ende verschlüsselt. Damit ist manchmal (im Fall der Nutzung von Android) sichergestellt, dass die übermittelten Rezeptdaten nur dem Empfänger (und nicht dem Dienst) zur Einsicht zur Verfügung stehen. Für den (üblichen) Fall, dass Rezeptdaten als Foto verschickt werden, wird momentan keine Verschlüsselung durch den Messenger angeboten. Dieser bekommt mindestens Kenntnis von der Telefonnummer des Apothekenkunden und die auf dem Handy gespeicherten Kontaktdaten. Dies passiert allerdings nicht im Auftrag der Apotheke, sondern ist dem Programm geschuldet. Es liest bei der Installation und eventuell auch zu einem späteren Zeitpunkt Kontaktdaten einfach aus. Die Metadaten der Kommunikation (die IP-Adressen beider Kommunikationspartner, Uhrzeit der Nachricht, Nutzer-IDs) werden in jedem Fall erfasst.

Aus diesen Gründen hielt der TLfDI das eben dargestellte Bestellverfahren für bedenklich und nahm eine Prüfung der Vereinbarkeit mit dem BDSG vor. Spätestens bei der Rückantwort des Apothekers über den Dienst wird jedoch gegen das in Deutschland geltende Datenschutzrecht verstoßen. Der Apotheker bedient sich dabei einer Übermittlungsart, deren technische und organisatorische Maßnahmen nicht dem notwendigen Maß entsprechen.
Die in der Anlage zu § 9 BDSG beschriebenen technischen und organisatorischen Maßnahmen sind zu erfüllen, da die Rezeptdaten unverschlüsselt auf dem Tablet-PC des Apothekers gespeichert werden. Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzepts zu ermitteln und haben je nach der Art der zu schützenden Daten zu gewährleisten,

1. dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Eigentlich ist seit den Enthüllungen von Edward Snowden, spätestens jedoch mit der EuGH-Entscheidung vom 6. Oktober 2015 (Az: C-362/14- siehe https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_unsafe_harbor.pdf; http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf) nun jedem deutlich vor Augen geführt worden, dass bei Datenübermittlungen in die USA

diese technischen und organisatorischen Maßnahmen nicht zu gewährleisten sind.
Technische und organisatorische Maßnahmen sind zum Schutz der personenbezogenen Daten, insbesondere bei Gesundheitsdaten, erforderlich. Können diese nicht gewährleistet werden, wie in diesem Fall, ist der Weg der Datenübermittlung datenschutzrechtlich unzulässig.
Es drängte sich insoweit auch die Frage auf, ob die Bereitstellung dieses Kommunikationsweges mit § 1 Abs. 1 der Berufsordnung der Landesapothekerkammer vereinbar ist. Danach ist der Apotheker verpflichtet, seinen Beruf gewissenhaft auszuüben und sich so zu verhalten, dass er dem entgegengebrachten Vertrauen seiner Patienten gerecht wird. Eine unzulässige Übermittlung von Patientendaten in die USA wird dem möglicherweise nicht gerecht.

Der TLfDI prüft derzeit die bestehenden Möglichkeiten, um diesen datenschutzrechtlich unzulässigen Teil des Verfahrens der Rezeptbestellung zu untersagen. Weiterhin wird der TLfDI mit der Apothekerkammer hierüber ins Gespräch kommen, um das Problem auf dieser Ebene für die Zukunft zu lösen.

Die Datenübermittlungen an Messengerdienste in die USA sind nach dem EUGH-Urteil zu „Safe Harbor“ unzulässig. Bietet ein Apotheker diesen Dienst an, so ist er auch für die Datensicherung und die damit verbundenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG verantwortlich. Da er diese aber nicht garantieren kann, ist die Rezeptbestellung auf diesem Weg insgesamt unzulässig! Dies gilt im Übrigen nicht nur für diesen Kommunikationsweg, sondern für die meisten über das Internet abgewickelten Bestellvorgänge ohne Verschlüsselung.

9.6 Verkauf von Apotheken-Kundendaten: Fragen Sie Ihren TLfDI!

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über eine unterbliebene Auskunft einer insolventen Apotheke A an den Betroffenen. Ein Auskunftsersuchen gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) dient dazu zu erfahren, welche personenbezogenen Daten eine verantwortliche Stelle, hier die Apotheke A, zu seiner Person gespeichert hat. Weiterhin soll mit einem solchen Auskunftsersuchen neben dem Zweck der Datenspeicherung auch in Erfahrung gebracht werden, welchem Empfänger personenbezogene Daten des Betroffenen ggf. weitergegeben wurden. Hintergrund der Anfrage war eine Werbemail der Apotheke B. Der Beschwerdeführer hatte ursprünglich eine Bestellung in der Online-Apotheke des Apothekengeschäfts A getätigt. Die Bestelldaten mussten dort für Abrechnungszwecke aufbewahrt werden.
Nach Ermittlung des Sachverhalts stellte sich der Hergang wie folgt dar: Wegen Zahlungsunfähigkeit wurde der Geschäftsbetrieb der Apotheke A aufgegeben. Zuerst wurde der Vertrieb über die Online-Apotheke eingestellt, ein halbes Jahr später dann auch das Apothekengeschäft vor Ort. In den Datenschutzbestimmungen der Apotheke A wird ausgeschlossen, dass die Kundendaten an Dritte weitergeben oder gar verkauft werden. Dennoch musste der TLfDI feststellen, dass alle Kunden- und Bestelldaten der Online-Apotheke sowie der Standortapotheke samt Server von dem rechtmäßig bestellten Insolvenzverwalter an die Apotheke B verkauft wurden. Dies mag zwar im Sinne der Insolvenzgläubiger sein, da der Insolvenzverwalter die Aufgabe hat, die Insolvenzmasse zu sichern und zu mehren, verstößt jedoch gegen datenschutzrechtliche Regelungen.
Eine Übermittlung, also Weitergabe, personenbezogener Daten ist nur erlaubt, wenn dies durch Gesetz geregelt ist oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Eine gesetzliche Grundlage für die Übermittlung der Kunden- und Bestelldaten der Apotheke A an die Apotheke B gibt es nicht. Auch gibt es keine besonderen datenschutzrechtlichen Regelungen für Insolvenzverwalter. Diese haben dieselben Regeln zu beachten wie auch der Betrieb, der von ihnen verwaltet wird. Folglich müsste für eine zulässige Datenübermittlung durch den Insolvenzverwalter die Einwilligung aller (!) Kunden vorliegen. Und zwar bevor er diese an die Apotheke B verkaufte. Die

Apotheke B hat sogleich Gebrauch von den unrechtmäßig erworbenen Daten gemacht und die Kunden der Online-Apotheke A beworben. Natürlich haben sich die Kunden der Online-Apotheke A gewundert, wie die Apotheke B an ihre Daten gelangt. Den TLfDI erreichten gleich mehrere Beschwerden darüber.
Der TLfDI hat im Laufe der Beschwerdebearbeitung festgestellt, dass die restlichen Server (die nicht verkauft wurden) von der Polizei für Ermittlungen sichergestellt wurden. Unter den sichergestellten Servern befindet sich auch der Server der E-Mail-Postfächer der Apotheke A. Der Inhaber der Apotheke A hat also keinerlei Möglichkeiten, die empfangenen E-Mails abzurufen. Das Auskunftsersuchen des Beschwerdeführers muss bis zum Abschluss der polizeilichen Ermittlungen unbeantwortet bleiben.
Nachdem der TLfDI die Apotheke B auf die unzulässige Datenerhebung hingewiesen hatte, wurden die Kundendaten der Online-Apotheke A gelöscht. Eine Bewerbung oder eine anderweitige Nutzung der Kundendaten der Online-Apotheke A erfolgte nicht mehr. Die übrigen Kundendaten der Apotheke A wurden gesperrt. Nach Abschluss der polizeilichen Ermittlungen sind die Kunden- und Bestelldaten sowie ausdrücklich besondere Arten personenbezogener Daten (Gesundheitsdaten der Patienten) an den Inhaber der Apotheke A zu übergeben. Dieser ist nämlich Berufsgeheimnisträger im Sinne des § 203 StGB. Daneben wurde ein Bußgeldverfahren gegen den Insolvenzverwalter der Apotheke A wegen unbefugter Verarbeitung nicht allgemein zugänglicher personenbezogener Daten eingeleitet.

Wenn keine gesetzliche Grundlage für eine Datenübermittlung an eine andere Stelle vorliegt, ist diese ohne die Einwilligung der Betroffenen nach § 4 Abs. 1 BDSG unzulässig. Die unzulässige Übermittlung von nicht allgemein zugänglichen personenbezogenen Daten kann mit einem Bußgeld in Höhe von bis zu 300.000 Euro geahndet werden.

9.7 Patientendaten: Hin und her, das ist nicht schwer. Aber rechtswidrig! – Weitergabe von Daten aus Labor

Ein Beschwerdeführer hatte sich beklagt, dass Laborleistungen über ein Drittunternehmen abgerechnet wurden, ohne dass er Kenntnis von der Beauftragung dieses Laborarztes durch seinen Hausarzt, geschweige denn von der Einschaltung einer Verrechnungsstelle

hatte. Im Zusammenhang mit einer Untersuchung hatte der Hausarzt einen Laborarzt beauftragt, vom Hausarzt entnommene Proben zu prüfen. Danach fand eine Datenübermittlung vom Hausarzt an den Laborarzt und eine Datenübermittlung vom Laborarzt an die Verrechnungsstelle statt.

Nach § 4 Bundesdatenschutzgesetz (BDSG) ist die Datenerhebung, Verarbeitung und Nutzung nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da weder das Bundesdatenschutzgesetz noch eine andere Rechtsvorschrift vorliegend einen Erlaubnistatbestand für die Datenweitergabe an die Verrechnungsstelle bereithielt, war zu prüfen, ob eine Einwilligung des Patienten den Hausarzt und den Laborarzt zur Weitergabe der Daten berechtigte.

Auf Nachfrage des TLfDI konnten jedoch weder der Hausarzt noch der Laborarzt eine Einwilligung des Patienten in die Weitergabe seiner Patientendaten an das abrechnende Drittunternehmen vorlegen. Die Versendung von Probenmaterial zu Untersuchungszwecken an ein medizinisches Labor stellte rechtlich gesehen die Weitergabe von personenbezogenen Patientendaten dar. Dasselbe galt für die Weitergabe von Patientendaten an eine externe Abrechnungsstelle durch den Laborarzt. Um eine derartige Weitergabe von Patientendaten vornehmen zu können, hätten die Patienten, über die Einwilligung hinaus, den Hausarzt von seiner Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB) entbinden müssen. Dieses gilt auch zwischen Berufsgeheimnisträgern selbst. Ein Arzt darf einem anderen Arzt keine Geheimnisse eines seiner Patienten verraten, nur weil der Kollege auch Arzt ist und somit unter dieselbe Schweigepflicht fällt. Dies ist zwar ein strafrechtliches Problem, weil sich der Arzt durch die Verletzung dieser Schweigepflicht unter Umständen strafbar macht, entfaltet jedoch auch im Datenschutzrecht Relevanz.

Die Patienten hätten zunächst dem Hausarzt eine Einwilligung in die Datenweitergabe an den Laborarzt erteilen und ihn von seiner Schweigepflicht entbinden müssen. Ebenso wie sie den Laborarzt von seiner Schweigepflicht hätten entbinden müssen.

Ein Auftragsdatenverarbeitungsvertrag zwischen dem Hausarzt und dem Laborarzt kam in dieser Konstellation nicht in Frage. Ein solcher Vertrag wird geschlossen, wenn ein Arzt personenbezogene Daten für sich selbst durch einen Dritten verarbeiten lassen möchte. Das Labor hingegen erbrachte eigene Leistungen und war insoweit auch nur bedingt dem Weisungsrecht des Arztes unterworfen. Teil-

weise musste das Labor seine eigenen Leistungen nach Gebührenordnung der Ärzte auch selber abrechnen. Daher handelte es sich beim Labor um eine eigene verantwortliche Stelle, der die besonderen Arten von personenbezogenen Daten nur unter der Maßgabe des § 28 Abs. 6 BDSG oder aufgrund einer Einwilligung nach § 4a BDSG übermittelt werden durften. Die Weitergabe der Patientendaten zu Abrechnungszwecken sowohl durch den Haus- als auch den Laborarzt an ein Abrechnungsunternehmen hingegen bedurfte eines Vertrages über die Auftragsdatenverarbeitung gemäß § 11 BDSG zwischen dem jeweiligen Arzt als Auftraggeber und dem Abrechnungsunternehmen als Auftragnehmer. Ansonsten hätte es sich um eine unbefugte Übermittlung von personenbezogenen Daten gehandelt. Besteht nun keine Entbindung von der Schweigepflicht und es werden dennoch Daten aufgrund eines solchen Vertrages weitergegeben, verstößt diese Weitergabe aufgrund des Vertrages gegen die ärztliche Schweigepflicht aus § 203 StGB. Dies wiederum führt zur Nichtigkeit des Vertrages über die Auftragsdatenverarbeitung, § 134 BGB, und damit auch zur datenschutzrechtlichen Rechtswidrigkeit der Datenweitergabe.
Nach intensivem Schriftverkehr wurde das Abrechnungsverfahren umgestellt. Das Labor rechnet nunmehr unmittelbar selbst gegenüber den Patienten ab. Die Weitergabe von Patientendaten an das abrechnende Drittunternehmen oder andere Abrechnungsgesellschaften erfolgt laut Angabe des Arztes und des Labors nicht mehr.

Bevor Ärzte die Patientendaten für Abrechnungszwecke an eine Verrechnungsstelle weitergeben, müssen die Patienten dem behandelnden Arzt eine Einwilligung in die Datenübermittlung vorlegen und den Arzt von der in § 203 StGB geregelten Schweigepflicht entbinden. Um eine wirksame Entbindung der Schweigepflicht zu erhalten, müssen die Patienten vor der Weitergabe ihrer Daten darüber informiert werden, wer diese erhält und wie mit diesen Daten weiter verfahren wird. Die Entbindung eines Arztes von der Schweigepflicht erfolgt seitens des Patienten immer freiwillig, kann aber konkludent erfolgen. Zu Nachweiszwecken sollte sich der Arzt dies aber quittieren lassen.

9.8 "Anonyme" Zufriedenheitsbefragung

Einem Patienten war von seiner Krankenkasse ein Fragebogen übersandt worden, in dem in anonymisierter Form einzelne ärztliche Leistungen aus Sicht des Patienten beurteilt werden sollten. Dies bezog sich unter anderem auf die Freundlichkeit des Personals, Wartezeiten vor der Behandlung und Ähnliches.
Bei einem späteren Arztbesuch staunte er nicht schlecht, als er einen Blick auf den PC-Bildschirm bei seinem behandelnden Arzt warf. Dort erkannte er den von ihm anonym ausgefüllten Fragebogen wieder, nur mit dem Unterschied, dass auf dem Fragebogen handschriftlich notiert sein Name stand.
Der Betroffene wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Überprüfung der Angelegenheit. Er hatte im Vertrauen darauf, dass es sich um eine anonyme Befragung handelte, seine positiven, aber auch negativen Einschätzungen abgegeben. Da er befürchtet, der Arzt könnte ihm das persönlich übel nehmen, bat er um Wahrung seiner Anonymität. Der TLfDI bat als Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz (BDSG) den behandelnden Arzt in allgemeiner Form um Auskunft, wie er in den Besitz von derartigen Fragebögen gekommen sei und wer die Namen von Patienten auf die Kopien ursprünglich anonymisierter Fragebögen geschrieben habe.
Der behandelnde Arzt teilte in aller Kürze mit, er erhalte von verschiedenen Krankenkassen pro Woche ca. 20 bis 30 personifizierte Fragebögen, zu denen er Stellung nehmen müsse. Selbstverständlich müsse er personenbezogen Stellung beziehen. Im Rahmen seiner medizinischen Stellungnahmen würden die Fragebögen dokumentiert. Gegen die personenbezogene Dokumentation von Fragebögen durch den Arzt als Grundlage für seine Stellungnahme an die Krankenkasse war aus datenschutzrechtlicher Sicht nichts einzuwenden, wenn hierfür entsprechende Schweigepflichtentbindungen der Patienten zur Antwort an die Krankenkassen vorlagen.
Wie es sich im konkreten Fall des Beschwerdeführers abgespielt hatte, konnte der TLfDI aufgrund der Wahrung der Anonymität des Beschwerdeführers letztendlich nicht herausfinden. Eine konkrete Nachfrage beim Arzt zu dem streitigen Fragebogen hätte den Beschwerdeführer offenbart. Daher blieben zwei Möglichkeiten der Bewertung: Entweder hatte ein Mitarbeiter der Krankenkasse den Namen des Beschwerdeführers auf den Fragebogen geschrieben oder

die Fragen waren so formuliert, dass es für den Arzt möglich war, die Identität des Beschwerdeführers zu erkennen und den Fragebogen der Patientenakte zuzuordnen.
In beiden Fällen lag die datenschutzrechtliche Verantwortlichkeit für die Wahrung der Anonymität der Patienten gegenüber dem Arzt bei der Krankenkasse. Hatte sie den Fragebogen mit dem Namen des Ausfüllers versehen, damit der Arzt hierzu personenbezogen Stellung beziehen konnte, begegnete dies erheblichen datenschutzrechtlichen Bedenken. Wird Patienten ein Fragebogen ausgehändigt, der den Anschein erweckt, es handle sich um eine anonyme Umfrage, gaukelt die Krankenkasse den Patienten vor, sie könnten hier ohne falsche Rücksicht auf den Arzt und im Vertrauen auf weitere „unbelastete“ Behandlung, Angaben machen. Später haut man aber die Patienten in die Pfanne, weil man klammheimlich den Namen des Ausfüllers auf den Bogen schreibt und dem Arzt zur Stellungnahme übersendet. Die nachträgliche Personifizierung von der Krankenkasse kann auf keine gesetzliche Rechtsgrundlage gestützt werden.
Wurde aus den auf dem Fragebogen gegebenen Antworten vom Arzt haarscharf auf den konkreten Patienten geschlossen, hat die Krankenkasse bei der Verfassung des Fragebogens den in § 3 Abs. 6 BDSG definierten Grundsatz nicht beachtet. Anonymisierung bedeutet das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Auch hierzu gibt es zwei Möglichkeiten, dem nachzukommen. Zum einen können die Fragen so gehalten werden, dass aus deren Antwort keine Einzelperson erkennbar ist. Kann dies nicht sichergestellt werden, müssen die Fragen statistisch aufbereitet werden, damit die Aussagen auf einen größeren Personenkreis zutreffen können. Hat ein Patient zum Beispiel eine seltene Erkrankung, könnte dem Hausarzt diese Angabe keinesfalls mitgeteilt werden, da er den Patienten sofort erkennen könnte. Handelt es sich um einen Facharzt, der nur solche seltene Erkrankungen behandelt, ist davon auszugehen, dass er unter seinen Patienten nicht ohne Weiteres den Ausfüller der Umfrage namhaft machen kann.
Die betreffende Krankenkasse hat ihren Sitz leider nicht im Zuständigkeitsbereich des TLfDI, sodass er der Angelegenheit unzuständigkeitshalber nicht weiter nachgehen konnte. Der TLfDI hat jedoch

die Aufsichtsbehörden der anderen Bundesländer im Hinblick auf Fragebogenaktionen der dort ansässigen Krankenkassen über die Feststellungen informiert.

Wird eine anonyme Umfrage durchgeführt, sollten sich die zur Ausfüllung der Fragebögen berufenen Betroffenen beigefügte Merkblätter und Hinweise genau ansehen und abschätzen, ob durch die verlangten Angaben ein Rückschluss auf die Person möglich ist. Den Betroffenen ist der Ablauf des Umgangs mit den Fragebögen zu erläutern. Ein anonym gestalteter Fragebogen darf nach Rückgabe an die ausgebende Stelle nicht durch Beschriftung mit dem Namen des Ausfüllers nachträglich personifiziert werden.

9.9 Datenschutz in Berufsausübungsgemeinschaften

Bei dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging im Berichtszeitraum die Beschwerde eines Patienten ein, der sich darüber beklagte, dass der Nachfolger seiner vorherigen Ärztin Kenntnis über seine gesamte Patientenakte hatte, ohne seine entsprechende Einwilligung.
Bei Ärzten handelt es sich um nicht-öffentliche Stellen, auf die nach § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) eben dieses Gesetz Anwendung findet. Das BDSG verzichtet auf eine abstrakte Umschreibung der nicht-öffentlichen Stellen. § 2 Abs. 4 Satz 1 BDSG zählt sie stattdessen auf: natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit diese nicht zu den öffentlichen Stellen des Bundes oder der Länder gehören.
Grundsätzlich ist die Verarbeitung und Nutzung personenbezogener Daten für diese Stellen nur zulässig, wenn dieses Gesetz oder eine andere Vorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Im hiesigen Fall stellte der TLfDI jedoch fest, dass die Herausgabe der Patientendaten an den Nachfolger der Ärztin aus datenschutzrechtlicher Sicht nicht zu beanstanden war. Der Nachfolger ist angestellter Arzt in einer überörtlichen Berufsausübungsgemeinschaft (ÜBAG). Ebenfalls zu dieser ÜBAG gehörte bis in das Jahr 2013 die frühere Ärztin des beschwerdeführenden Patienten. Somit handelte es sich nach Feststellung des TLfDI vorliegend um keine Arztpraxisübernahme. Bei einer Praxisübernahme wird oft auf das so genannte Zwei-Schränke-

Modell zurückgegriffen. Dabei werden die übernommenen Patientenakten zunächst separat im „ersten Schrank aufbewahrt“. Sobald die Einwilligung der Patienten vorliegt, werden die Akten dann in das laufende System und somit in den „zweiten Schrank“ der übernehmenden Praxis eingefügt. Diese Bewertung hat der TLfDI bereits in seinem 1. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich unter der Nummer 3.33 (Bis zur Bahre: Patientenakten am Ende) vorgenommen. An dieser Bewertung hat sich auch in diesem Berichtszeitraum nichts geändert.
Bei einer Berufsausübungsgemeinschaft handelt es sich um einen rechtlich verbindlichen Zusammenschluss von Ärzten zur gemeinsamen Ausübung der ärztlichen Tätigkeit (z. B. die "Gemeinschaftspraxis"). Die berufsrechtliche Legitimation einer ÜBAG bildet § 18 Abs. 3 Satz 3 Muster-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO). Diese Besonderheit der Gemeinschaftspraxis muss nach außen, also insbesondere gegenüber den Patientinnen und Patienten, eindeutig erkennbar sein. Grundsätzlich schließen die Patienten bei einer solchen Berufsausübungsgemeinschaft mit allen Ärzten gemeinschaftlich einen Behandlungsvertrag.
Aufgrund dieses gemeinschaftlichen Behandlungsvertrages sind die Ärzte in einer solchen ÜBAG zur wechselseitigen Behandlung berechtigt und insoweit auch von der ärztlichen Schweigepflicht befreit. Seitens der ÜBAG erfolgt eine gemeinsame Dokumentation und damit verbunden auch ein gemeinsamer Datenbestand, auf den jeder der ÜBAG angeschlossene Arzt bei Erforderlichkeit zugreifen darf.
Nach Vorgenanntem durfte daher auch der Nachfolger der Ärztin auf die alte Patientenakte zugreifen. Ein Widerspruch des Patienten lag nicht vor.

Bei einer Berufsausübungsgemeinschaft (BAG) handelt es sich um einen rechtlich verbindlichen Zusammenschluss von Ärzten zur gemeinsamen Ausübung der ärztlichen Tätigkeit (z. B. die "Gemeinschaftspraxis"), vergleiche § 18 Abs. 3 Satz 3 (Muster-) Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO). Die Patienten schließen bei einer solchen Berufsausübungsgemeinschaft mit allen Ärzten gemeinschaftlich einen Behandlungsvertrag. Dabei erfolgt eine gemeinsame Dokumentation und damit verbunden auch

ein gemeinsamer Datenbestand, auf den jeder der BAG angeschlossene Arzt bei Erforderlichkeit zugreifen darf.

9.10 Zugriffsrechte der Geschäftsführung eines Krankenhauses auf Patientendaten

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage eines externen Datenschutzbeauftragten eines Krankenhauses in privater Trägerschaft, inwieweit der Zugriff der Geschäftsführung auf Patientendaten zulässig sei. Vor allem ging es ihm um die datenschutzrechtliche Auskunft, ob auch von außen kommende Faxe (Laborbefunde, Arztbriefe usw.) an die Geschäftsführung versandt werden durften.
Generell gilt, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur dann zulässig ist, soweit ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Daten über den Gesundheitszustand sind äußerst sensible Daten, die das BDSG zu den besonderen Arten personenbezogener Arten zählt, vergleiche § 3 Abs. 9 BDSG. Da es sich hier um ein Thüringer Krankenhaus handelte, sind die Regelungen des Thüringer Krankenhausgesetzes (ThürKHG) als lex specialis vorrangig vor dem BDSG.
Nach § 27 Abs. 10 Satz 1 ThürKHG hat das Krankenhaus die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der in den Absätzen 1 bis 9 enthaltenen Bestimmungen zu gewährleisten. Danach dürfen nach § 27 Abs. 3 Satz 1 Nr. 1 THürKHG Patientendaten nur erhoben, gespeichert, verändert oder sonst genutzt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist.
Die Mitteilung von Patientendaten innerhalb des Krankenhauses im Rahmen der Behandlung, zur Abwicklung des Behandlungsvertrages sowie zur Patientendokumentation stellt keine unbefugte Offenbarung von Patientengeheimnissen und keine unzulässige Datenweitergabe dar. Voraussetzung ist, dass die Krankenhausmitarbeiter hinsichtlich der Datenverarbeitung den Weisungen des ärztlichen Direktors bzw. des leitenden Arztes unterliegen und die Mitteilung der Daten im Rahmen des Behandlungsverhältnisses erforderlich ist. Diese Datennutzung durch berufsmäßig tätige Gehilfen bewegt sich

im Rahmen der datenschutzrechtlichen Zweckbindung. Anders ist die Mitteilung an Externe, also solche Personen, die nicht zum Krankenhaus und damit nicht zum Behandlungsteam gehören (z. B. externe Labor- und Konsiliarärzte). Deren Einschaltung ist nicht selbstverständlich; mit ihr muss der Patient nicht rechnen. Daher bedarf es für deren Einschaltung der Einwilligung des Patienten, vergleiche § 27 Abs. 3 Satz 1 Nr. 4 ThürKHG. Eine wirksame Einwilligung setzt voraus, dass der Patient weiß, wem erlaubt wird, welche Daten zu welchem Zweck zu verarbeiten sind. Die Erklärung muss freiwillig erfolgen; über etwaige Folgen der Nichteinwilligung ist zu informieren. Nach § 27 Abs. 3 Satz 2 ThürKHG bedarf die Einwilligung in jedem Einzelfall der Schriftform, soweit nicht wegen besonderer Umstände des Einzelfalls eine andere Form angemessen ist.

Anders liegt der Fall bei vor- und nachbehandelnden Ärzten, dort wird die Einwilligung der Patienten hinsichtlich der Übersendung des Entlassungsbefundes, aus dem sich die für die Nachbehandlung notwendigen therapeutischen Konsequenzen ergeben, unterstellt.

Im Ergebnis teilte der TLfDI dem externen Datenschutzbeauftragten mit, dass es für die Datenübermittlung immer der Einwilligung der Patienten bedurfte, soweit die Geschäftsführung nicht zum Behandlungsteam des Krankenhauses gehörte. Weitere Informationen zu Zugriffsrechten auf das Krankenhausinformationssystem und die elektronische Patientenakte sind in der Orientierungshilfe Krankenhausinformationssysteme auf der Website des TLfDI unter https://www.tlfdi.de/imperia/md/content/datenschutz/themen/gesundheit/oh_kis_v2_korr.pdf zu finden.

Im Rahmen einer Krankenhausbehandlung müssen oft externe Personen und Stellen über bestimmte Angaben der Patienten unterrichtet werden. Generell gilt, dass solche Datenübermittlungen nur zulässig sind, wenn der betroffene Patient hierin wirksam eingewilligt hat oder wenn für diese Übermittlung eine explizite gesetzliche Grundlage besteht, vergleiche § 27 ThürKHG.

9.11 Dr. jur. Hasse wird zu Dr. med. Hasse

Bass erstaunt war der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), als er unter seiner Privatadresse von einem Krankenhaus angeschrieben wurde und ihm als „Kollegen“ ein Arztbrief (Anamnese samt einer Diagnose in Kurzfassung sowie detaillierte Untersuchungsbefunde) zu einem Patienten des Krankenhauses zugesandt wurde. Dieser Vorgang wiederholte sich.

Umgehend antwortete der TLfDI dem Krankenhaus und informierte darüber, dass er nicht der korrekte Adressat des versandten Briefes sei. Aus Sicht des TLfDI war dieses Vorkommnis besorgniserregend und führte zu der Schlussfolgerung, dass dem Datenschutz in diesem Fall nicht mit der Sorgfalt begegnet worden war, die der Gesetzgeber für besondere Arten von personenbezogenen Daten wie Gesundheitsdaten für angemessen erachtet hat. Er richtete daher ein Auskunftsersuchen an das Krankenhaus und bat um Mitteilung, ob ein Datenschutzbeauftragter bestellt sei. Weiterhin wollte er wissen, welche technischen und organisatorischen Maßnahmen getroffen worden waren, damit besondere Arten personenbezogener Daten nicht in falsche Hände geraten. Insbesondere sollte dargelegt werden, wie Adressen von Hausärzten, denen Arztbriefe übersandt werden sollen, recherchiert werden und ob das verantwortliche Personal geschult wird, um Fehlsendungen auszuschließen.

Die Klinik teilte mit, dass zu diesem Vorfall nach dem Gespräch mit der betreffenden Sekretärin ein persönliches Fehlverhalten festgestellt werden konnte. In der betreffenden Patientenakte befand sich eine Schweigepflichtsentbindung des Patienten für Datenübermittlungen an seinen Hausarzt. Der Hausarzt hat einen ähnlich klingenden Nachnamen wie der TLfDI und wohnt in einem ähnlich klingenden Ort. Die Sekretärin hatte den Eintrag des Hausarztes im Krankenhausinformationssystem nicht gefunden. Daher hatte Sie eine Internetsuche durchgeführt, war auf den Namen des TLfDI gestoßen und hatte diesen für den Hausarzt gehalten. Richtig wäre in diesem Fall gewesen, im Intranet in der Datenbank der kassenärztlichen Vereinigung Thüringen zu recherchieren. Dort hätte sie den Hausarzt finden können. Aufgrund dieses Fehlverhaltens der Sekretärin wurden die Mitarbeiterinnen des Schreibdienstes sofort von dem betrieblichen Datenschutzbeauftragten (bDSB) schriftlich belehrt; eine erneute Schulung fand zeitnah statt.

Die vom Krankenhaus getroffenen technischen und organisatorischen Maßnahmen zur Adressfindung der Ärzte waren datenschutzgerecht. In diesem Fall hatte sich aber eine Mitarbeiterin nicht daran gehalten und wollte auf einem schnellen Weg eine pragmatische Lösung erzielen.

Auch wenn eine verantwortliche Stelle alle zur Einhaltung des Datenschutzes erforderlichen technischen und organisatorischen Maßnahmen trifft, gibt es immer noch den „Faktor Mensch“, der die personenbezogenen Daten verarbeitet. Damit sich die Mitarbeiter an die getroffenen Vorgaben halten, sind regelmäßige Unterweisungen durch den betrieblichen Datenschutzbeauftragten geboten.

9.12 Taubenschlag Stationszimmer

Ein Bürger wandte sich anonym an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er teilte mit, dass er seine Frau in einem Krankenhaus in Thüringen besucht habe. Dabei habe er feststellen müssen, dass es dort mit dem Datenschutz wohl nicht so genau genommen würde. Man habe einfach in das unverschlossene Stationszimmer gehen können und dort sei niemand anwesend gewesen. Man hätte also problemlos Patientenunterlagen zur Kenntnis nehmen können. Der TLfDI wandte sich an das Krankenhaus und bat um Mitteilung, welche Festlegungen dort im Hinblick auf den Datenschutz getroffen worden seien, insbesondere wie sichergestellt werde, dass Unbefugte keinen Zugriff bzw. keine Einsicht in Patientenunterlagen erhalten. Das Krankenhaus teilte über seinen externen Beauftragten für den Datenschutz mit, dass in den Stationszimmern, wie in jedem anderen Krankenhaus auch, Akten, Therapiepläne, Medikationspläne, Belegungspläne usw. aufbewahrt würden. Der Datenschutzbeauftragte habe bei einer jüngst durchgeführten Unterweisung sowohl dem ärztlichen als auch dem Stationspersonal nochmals deutlich gemacht, welchen wichtigen Stellenwert der Datenschutz habe. Hierzu sei auch eine Dienstanweisung in Vorbereitung. Darin solle geregelt werden, dass Diensträume ohne anwesendes Personal verschlossen zu halten sind. Auch dem Patienten solle klar sein, dass er als Unbefugter keinen Zugang zu Stationszimmern habe. Dies wurde im Patientenmerkblatt zum Datenschutz formuliert.

Nach § 27 Abs. 10 Thüringer Krankenhausgesetz hat das Krankenhaus die technischen und organisatorischen Maßnehmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der im Krankenhausgesetz enthaltenen Bestimmungen zum Datenschutzgesetz einzuhalten. Da das Krankenhaus danach verpflichtet ist, alle wesentlichen Regelungen zum Datenschutz schriftlich festzuhalten, wurde das Krankenhaus aufgefordert, die in Aussicht gestellte Dienstanweisung dem TLfDI zur Prüfung vorzulegen. Der TLfDI stellte fest, dass das für die Klinik erstellte Handbuch zum betrieblichen Datenschutzsystem nunmehr auch die Festlegungen enthielt, die zum Schutz der Patientendaten im Stationszimmer erforderlich sind. Es enthält Festlegungen zum Umgang mit Telefaxgeräten, zur Benutzung von Computern, zum Löschen von Patientendaten und vieles mehr. Festgelegt worden ist auch, dass beim Verlassen des Arbeitsplatzes der Bildschirm auf die Anmeldemaske zu stellen ist oder die benutzerspezifischen Programme geschlossen werden müssen. Bei längerem Fernbleiben vom Arbeitsplatz sind alle Anwendungen zu schließen und der Computer ist herunterzufahren. Zugänge zu Stationszimmern, Untersuchungsräumen und Büros sind grundsätzlich geschlossen zu halten und bei längerer Abwesenheit abzuschließen. Weiterhin müssen Diensträume verschlossen werden, wenn sich niemand in ihnen aufhält. Die Visitenwagen müssen, wenn sie auf dem Flur stehen, verschlossen sein, um zu gewährleisten, dass kein Zugriff auf die Akten durch nicht autorisierte Personen möglich ist.
Damit waren die wesentlichen datenschutzrechtlichen Festlegungen getroffen. Werden sie eingehalten, können damit unbefugte Zugriffe auf Patientendaten ausgeschlossen werden.

Krankenhäuser müssen schriftliche Festlegungen dazu treffen, wie der Datenschutz in ihrem Haus einzuhalten ist. Erforderlich sind hierzu insbesondere auch Regelungen zur Zutrittsberechtigung zu Räumen oder zur Einsichtnahme in Patientenunterlagen.

9.13 Mögliche Straftat wegen Versendung des ärztlichen Abschlussbefunds

Ein Bürger beschwerte sich per E-Mail beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den Arzt eines Krankenhauses wegen unzulässiger Übermittlungen des Abschlussbefunds an verschiedene Adressaten. Der Beschwerdeführer berichtete ergänzend, dass er bei der Patientenaufnahme eindeutig festgelegt habe, wer den Abschlussbefund erhalten durfte. Der TLfDI bat den Beschwerdeführer zunächst für die weitere Kommunikation um die Mitteilung seiner Postanschrift, da die unverschlüsselte Übermittlung von personenbezogenen Informationen als E-Mail im Internet mit erheblichen datenschutzrechtlichen Risiken verbunden ist. Eine unverschlüsselte E-Mail ist weder gegen die Kenntnisnahme durch Unbefugte noch gegen eine inhaltliche Veränderung geschützt. Der Bürger wurde weiterhin darüber informiert, dass der von ihm geschilderte Sachverhalt möglicherweise eine Straftat nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) wegen Verletzung des Patientengeheimnisses darstellt. Für die Verfolgung derartiger Straftaten ist der TLfDI nicht zuständig. In den Fällen des § 203 StGB wird die Tat nur auf Antrag verfolgt, wobei der Antragsberechtigte den Antrag bis zum Ablauf einer Frist von drei Monaten stellen muss, da diese danach nicht mehr verfolgt wird. Die Anzeige einer Straftat und der Strafantrag können bei der Staatsanwaltschaft, den Behörden und Beamten des Polizeidienstes und den Amtsgerichten mündlich oder schriftlich angebracht werden. Der Beschwerdeführer wurde gebeten, sofern er eine datenschutzrechtliche Prüfung der Angelegenheit wünscht, dem TLfDI sein Einverständnis mitzuteilen, dass dem Krankenhaus gegenüber sein Name genannt werden darf. Eine Reaktion seitens des Beschwerdeführers erfolgte daraufhin jedoch nicht mehr.

Für die Verfolgung von Straftaten im Zusammenhang mit der Verarbeitung oder Nutzung personenbezogener Daten ist der TLfDI nicht zuständig. Die Anzeige einer Straftat und der Strafantrag sind bei der Staatsanwaltschaft, den Behörden und Beamten des Polizeidienstes und den Amtsgerichten mündlich oder schriftlich heranzutragen.

9.14 Pflegeheim in kirchlicher Trägerschaft – der TLfDI muss draußen bleiben

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) kontaktierte ein besorgtes Familienmitglied eines Pflegeheimbewohners. Es teilte mit, dass in diesem Pflegeheim eine Pflegekraft eingestellt sei, welche mehrfach das Gebot der Verschwiegenheit verletzt haben soll. Im weiteren Gespräch stellte sich aber heraus, dass dieses Pflegeheim eine kirchliche Einrichtung ist. Dem Familienmitglied wurde mitgeteilt, dass der TLfDI gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz kontrolliert und gemäß § 42 ThürDSG in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) zwar Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen ist. Aber eine Zuständigkeit des TLfDI für dieses Pflegeheim war aufgrund des verfassungsrechtlich garantierten Selbstbestimmungsrechts von Religionsgemeinschaften nicht gegeben. Das BDSG gilt im Bereich der kirchlichen Einrichtungen nicht. Die Evangelische Kirche in Deutschland und die Bistümer der Katholischen Kirche in Deutschland haben eigene Datenschutzvorschriften erlassen (die evangelische Kirche beispielsweise das Datenschutzgesetz der Evangelischen Kirche in Deutschland [DSG-EKD]) und haben auch eigene Datenschutzbeauftragte.
Mit Einverständnis des Familienmitgliedes wurde diese Anfrage an die für Thüringen zuständige Stelle, den Datenschutzbeauftragten des Diakonischen Werkes Evangelischer Kirchen in Mitteldeutschland e. V., Ingenieurbüro für Datenschutz und Datensicherheit, Dipl.-Ing. P.-G. Große, Albrecht-Thaer-Straße 5 in 09117 Chemnitz, zur weiteren Bearbeitung übersandt und dort weiter bearbeitet.

Aufgrund des verfassungsrechtlich garantierten Selbstbestimmungsrechts von Religionsgemeinschaften gilt das Bundesdatenschutzgesetz im Bereich der Kirchen nicht. Die Evangelische Kirche in Deutschland und die Bistümer der Katholischen Kirche in Deutschland haben eigene Datenschutzvorschriften erlassen und eigene Datenschutzbeauftragte. Entsprechende Anfragen werden, bei Einverständnis des Betroffenen, an diese zuständige Stelle zur weiteren Bearbeitung übersandt.

9.15 Daten am Arm – in Ordnung oder nicht? – Zur Zulässigkeit von Patientenarmbändern

Krankenhäuser müssen sparen und trotzdem die Versorgung ihrer Patienten sicherstellen. Dazu gehört natürlich, dass jeder Patient genau die Behandlung erhält, die er braucht und nicht jene, die für seinen Bettnachbarn vorgesehen ist. Beide Aspekte mögen dafür sprechen, dass Kliniken Patientenarmbänder einführen, die persönliche Daten des Patienten beinhalten und elektronisch ausgelesen werden können. Auch Thüringer Kliniken setzen sie ein, um Verwechslungen entgegenzuwirken und um Betriebsabläufe zu optimieren. Ob es dabei datenschutzgerecht zugeht, prüfte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem die Presse über die Einführung solcher Bänder an einer namhaften Klinik berichtete. Die Geschäftsführung wurde vom TLfDI angeschrieben und um nähere Angaben zum Verfahren gebeten. Dabei war zunächst von Interesse, welche Daten genau auf dem Patientenarmband abgespeichert werden und zu welchem Zweck. Ferner wurde erfragt, wie mit den Armbändern bei Entlassung umgegangen wird und welche Maßnahmen bei Verlust greifen. Eine zentrale Frage war natürlich auch, ob und in welcher Weise ein Patient in die Verwendung des Bandes einwilligen kann. Letzteres wäre eine zwingende Voraussetzung für seine Zulässigkeit nach § 4 Abs. 1 Bundesdatenschutzgesetz, denn eine Rechtsvorschrift, die eine derartige Verarbeitung und Nutzung von personenbezogenen Daten von Patienten erlaubt bzw. anordnet, gibt es nicht. Die Geschäftsführung antwortete fristgerecht und umfassend. Dabei wurde klar, dass jeder Patient schriftlich über den Umfang der gespeicherten Daten sowie den Zweck des Armbandes aufgeklärt wird und seine Zustimmung zur Verwendung des Bandes erteilen oder diese verweigern kann. Auch ein Hinweis, dass das Band nach Entlassung des Patienten datenschutzgerecht entsorgt werde, ist auf dem Informationsblatt für den Patienten enthalten. Der TLfDI reagierte mit einem abschließenden Schreiben an die Geschäftsführung mit beratenden Hinweisen.

Maßnahmen zur Verbesserung von Effizienz und Sicherheit in Krankenhäusern dürfen nicht zu Lasten des Patientendatenschutzes gehen. Eine Überprüfung des TLfDI ergab erfreulicherweise, dass Armbänder, auf denen die persönlichen Daten des Patienten elektronisch

gespeichert sind, datenschutzkonform eingesetzt werden. Der Patient kann ihrer Verwendung zustimmen oder diese ablehnen. Nach Entlassung werden die Bänder datenschutzgerecht entsorgt.

9.16 Hinter den Kulissen einer Apotheke

Alle Jahre wieder. Auch in diesem Berichtszeitraum kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Apotheken. Denn wieder einmal beschwerte sich ein Kunde beim TLfDI, dass er in einer öffentlich zugänglichen Mülltonne einer Apotheke ungeschredderte Kassenbons mit Kundendaten inklusive der Medikationen gefunden hätte. Dieser Vorwurf bestätigte sich bei einer Kontrolle der Apotheke durch den TLfDI nicht.
Dennoch stellte der TLfDI im Rahmen der Kontrolle fest, dass die von der Apotheke verwendeten Schredder nicht der nötigen Sicherheitsstufe entsprachen. Gerade in Apotheken wird täglich mit hochsensiblen Patientendaten i. S. d. § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG), die aufgrund ihrer Schutzbedürftigkeit einem sehr hohen Vertraulichkeitsgrad unterfallen, gearbeitet. Solche Daten, welche Rückschlüsse auf bestimmte oder zumindest bestimmbare Personen zulassen, dürfen keinesfalls nur zerrissen oder grob geschreddert werden. Es ist vielmehr notwendig, dass diese Dokumente und Rezepte stets so geschreddert werden, dass eine Widerherstellung des Inhalts dauerhaft unmöglich gemacht wird und die einzelnen Papierstücke in keinen Zusammenhang mehr gebracht werden können. Die Geräte zum Schreddern solcher Dokumente müssen mindestens nach der alten DIN-Norm 32757 die Sicherheitsstufe 4 bzw. nach der neuen DIN 66399-1 mindestens die Sicherheitsstufe P-5 aufweisen. Dies ergibt sich aus der Datensicherheitsvorschrift § 9 BDSG. Danach müssen nicht-öffentliche Stellen, wie Apotheken, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetztes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.
Weiterhin entdeckten die Mitarbeiter des TLfDI bei der Kontrolle der Geschäftsräume der Apotheke eine Vielzahl von Videokameras, die jeweils technisch in unterschiedlichem Zustand waren. Teils waren die Domekameras deinstalliert oder es war nur für jedermann

sichtbar ein leeres Gehäuse angebracht. So insbesondere hinter dem Verkaufstresen wie auch im Vorraum zur Apotheke. Ebenfalls stellte der TLfDI im Rahmen der Begehung fest, dass die Kameratechnik, insbesondere das zentrale Aufzeichnungsgerät, nicht angeschlossen war. Dieses Aufzeichnungsgerät bewahrte die Apotheke unangeschlossen im Büro auf. Der TLfDI erteilte der Apotheke den Hinweis, dass auch von nicht betriebenen Kameras derselbe Überwachungsdruck für den Betroffenen ausgehe wie von den funktionierenden Modellen. Der Betroffene hat in diesem Fall keine Möglichkeit, den Betriebszustand zu erkennen. Daher werden ausgeschaltete Kameras oder Kameraattrappen nach denselben rechtlichen Grundsätzen behandelt wie eine tatsächlich betriebene Kamera. Im hiesigen Fall ist die einschlägige Erlaubnisnorm § 6b BDSG. Diese regelt den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen. Zu solchen zählt auch der Verkaufsraum einer Apotheke, da er einem nicht näher bestimmbaren Personenkreis zugänglich ist und der Betreiber sogar möchte, dass die Kundschaft die Räumlichkeiten betritt.
Die vom TLfDI mitgeteilten Voraussetzungen wurden vom kooperativen Unternehmen umgesetzt. So wurden die ohnehin nicht betriebenen Kameras ausgebaut und neue Schredder angeschafft. Das Verfahren war damit abgeschlossen.

Hochsensible Patientendaten müssen stets so geschreddert werden, dass eine Wiederherstellung des Inhalts dauerhaft unmöglich gemacht wird und die einzelnen Papierstücke in keinen Zusammenhang mehr gebracht werden können, vergleiche DIN66399-1. Ausgeschaltete Kameras oder Kameraattrappen werden nach denselben rechtlichen Grundsätzen behandelt wie eine tatsächlich betriebene Kamera.

9.17 Personalausweiskopie in der Arztpraxis?

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit war dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt geworden, dass in einer Arztpraxis Kopien bzw. Scandokumente des Bundespersonalausweises der Patienten angefertigt wurden. Zweck der Personalausweiskopie war es, die Rechnung an die richtige Adresse zuzustellen, wenn die Krankenkassenkarte vom Patienten nicht vorgelegt werden konnte.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten war nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsnorm dies erlaubte oder der Betroffene eingewilligt hatte, § 4 Abs. 1 BDSG. Nach § 28 Abs. 1 Nr. 2 BDSG war das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der Arztpraxis erforderlich war und kein Grund zu der Annahme bestand, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwog. Jedenfalls durfte nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich durch öffentliche und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20 PAuswG erfolgen. In der Gesetzesbegründung zu § 14 PAuswG hieß es: „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die vorgesehenen Wege erfolgen darf. (…) Weitere Verfahren, z. B. über die opto-elektronische Erfassung (‚scannen') von Ausweisdaten oder den maschinenlesbaren Bereich, sollen ausdrücklich ausgeschlossen werden." (BR-Drs. 550/08, S. 69 f.).
Zu Identifikationszwecken bedarf es grundsätzlich nur der Überprüfung der Stammdaten wie Name und Anschrift (siehe auch Beitrag Nummer 2.7) Daten, die nicht zur Identifizierung benötigt wurden, durften nicht erhoben werden. Dies galt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Angabe der Personalausweisnummer war grundsätzlich ebenfalls nicht erforderlich. Eine Alternative zur Personalausweiskopie zum Zweck der Identifikationsfeststellung stellte das Aufzeichnen des Namens und der Anschrift dar. Dies konnte in der üblichen Weise erfolgen, indem diese Daten aus dem vorgelegten Personalausweis notiert wurden. Der Personalausweis war anschließend den Patienten zurückzugeben.
Die Arztpraxis kam den Aufforderungen des TLfDI nach.

Zur Identifikationsfeststellung einer Person bedarf es grundsätzlich nur der Erhebung des Namens und der Anschrift. Eine Kopie des Personalausweises ist unzulässig.

9.18 Klinische Studien – nicht ohne Datenschutz

Klinische Studien werden in Deutschland oft bundesweit bzw. in mehreren Ländern durchgeführt. Um die Verhältnisse im Vorfeld abzuklären, wenden sich des Öfteren Stellen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um die in Thüringen geltenden Modalitäten in Erfahrung zu bringen. So auch ein privates Studienzentrum, das wissen wollte, ob es zulässig sei, dass medizinische Daten (Laborwerte, Röntgenbilder, MRT Ergebnisse, Arztbriefe etc.), die im Rahmen einer medizinischen Studie erhoben wurden, an ein nicht-öffentliches Unternehmen zur Weiternutzung weitergeleitet werden, wenn der Studienpatient im Detail über die Nutzung der Daten aufgeklärt, dieses dokumentiert wurde und der Patient sich einverstanden erklärt hatte. Dabei sollte der Patient zwar über die genaue Weiterverwendung und Nutzung seiner Daten aufgeklärt werden, die Daten dann aber auch studienübergreifend und auch für andere Zwecke genutzt werden. Daneben sollte der Patient seine Daten auch selbst erhalten. Außerdem sollte der TLfDI darlegen, welches Gesetz einschlägig ist und welche Regularien für die Übermittlung und Weiterverwendung von Daten von Studienpatienten gelten, die nicht aus Deutschland, sondern aus anderen Ländern der EU kommen, und unter welchen Voraussetzungen die Datenübermittlung und Weiterverwendung von medizinischen Daten von Patienten in den USA möglich ist.

Der TLfDI legte dar, dass gemäß § 4 Bundesdatenschutzgesetz (BDSG) die Verarbeitung und damit nach § 3 Abs. 4 Satz 1 BDSG auch die Übermittlung von personenbezogenen Daten nur zulässig ist, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei Gesundheitsdaten, die als so genannte besondere Arten personenbezogener Daten einem besonderen Schutz unterliegen, ist nach § 4a Abs. 3 BDSG eine Einwilligung einzuholen, die sich ausdrücklich auf diese Daten bezieht. Darüber hinaus ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, § 4a Abs. 1 Satz 1 BDSG, und er hinreichend informiert wurde, § 4a Abs. 1 Satz 2 BDSG.

Bei Einholung der Einwilligung muss der Zweck der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten feststehen und der Betroffene muss hierüber informiert werden, § 4a Abs. 1 Satz 2 BDSG. Aus der Einwilligung ergibt sich gerade nicht die

Befugnis, die Daten für andere Zwecke zu nutzen. Aus datenschutzrechtlicher Sicht bestehen grundsätzlich keine Vorbehalte gegen die Bekanntgabe medizinischer Studiendaten an den betroffenen Patienten selbst (sofern kein Bezug zu Dritten besteht). Den Betroffenen steht sogar ein Auskunftsanspruch nach § 34 BDSG hinsichtlich der zu ihrer Person gespeicherten personenbezogenen Daten zu.
Der TLfDI stellte zudem klar, dass es nicht auf die Nationalität des Patienten, sondern darauf ankommt, von welcher Stelle die Daten wo erhoben werden. Da es sich bei den USA um einen Staat außerhalb des Europäischen Wirtschaftsraums handelt, sind bei Datenübermittlungen die Vorgaben der §§ 4b, 4c BDSG bzw. §§ 23 Thüringer Datenschutzgesetz maßgeblich. Der anfragenden Stelle wurde mitgeteilt, dass für die USA ein angemessenes Datenschutzniveau nicht anerkannt ist (vergleiche hierzu Beitrag 2.1 zu der „Safe-Harbor-Entscheidung“ des EuGH Nr. C-362/14) und daher eine Übermittlung von Gesundheitsdaten in die USA nicht zulässig ist. Die anfragende Stelle hat sich nicht wieder gemeldet.

Vor der Durchführung von klinischen Studien wenden sich die verantwortlichen Stellen des Öfteren an den TLfDI, um die in Thüringen geltende Rechtslage in Erfahrung zu bringen. Der TLfDI ist zur Erteilung von Auskünften gern bereit. Gesundheitsdaten unterliegen als so genannte besondere Arten personenbezogener Daten einem besonderen gesetzlichen Schutz. Es gelten erhöhte Anforderungen an die Einwilligung des Studienteilnehmers zur Verarbeitung seiner Daten.

9.19 Ist die Arztqualifikation auch echt?

Sie kennen das sicher: Beim Arztbesuch in der Arztpraxis hängen häufig Urkunden und Fortbildungszertifikate zu Qualifikationen oder zusätzlichen Spezialisierungen und Lehrgängen. Dadurch wird dem Patienten angezeigt, welche Leistungen in der Praxis qualifiziert durch den Arzt oder durch das medizinische Fachpersonal durchgeführt werden können. Doch, woher weiß der Patient, dass ein solches Fortbildungszertifikat auch echt ist?
Um dem Bürger die Möglichkeit zu geben, dies schnell und einfach prüfen zu können, betreibt die Landesärztekammer Thüringen mit anderen Ärztekammern ein Online-Portal bei der Bundesärztekammer https://www.kammerservice.de/, mit welchem die Prüfung die-

ser Urkunden möglich ist. Dafür ist auf der Urkunde ein QR-Code abgedruckt, der eine 64-stellige Zeichenfolge enthält. Diese Zeichenfolge ist die eindeutige Urkundennummer. Gibt man die Zeichenfolge, welche man sich zuvor beim Arzt notiert oder etwa als Handyfoto gespeichert hat, in dem o. g. Portal ein, werden die Daten, welche auf der Urkunde abgedruckt sind, auch online angezeigt. So kann die Urkunde auf Echtheit überprüft werden.

Um diese Überprüfung technisch zu ermöglichen, werden hierzu die Daten von Urkunden und Fortbildungszertifikaten dezentral in den jeweiligen Landesärztekammern vorgehalten. Das Online-Portal, welches über die Bundesärztekammer betrieben wird, leitet die elektronischen Anfragen an die zuständigen Ärztekammern weiter. Anhand des Codes erkennt das Portal die zuständige Landesärztekammer.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte sich über die technische Sicherung der Zugänge, was insbesondere die Transportverschlüsselung vom Nutzer zum Portal-Server betraf. Außerdem wurde die Landesärztekammer Thüringen bezüglich der Bildungsregeln der Urkundennummer beraten. Hierbei war es vor allen Dingen wichtig, dass die Nummer, welche unter anderem aus dem Namen des Urkundeninhabers und weiteren Urkundendaten gebildet wird, nicht doppelt vorkommen darf, um die Eindeutigkeit der Urkunden zu gewährleisten. Hinsichtlich des Verfahrens in Thüringen steht der TLfDI mit der Landesärztekammer weiterhin in Kontakt, um die Sicherheit des Verfahrens abschließend beurteilen zu können. Das Verfahren selber befindet sich noch in der Testphase.

Wollen Bürger zukünftig die Echtheit einer Urkunde oder eines Fortbildungszertifikates vom Arzt- oder Medizinischen Fachpersonal prüfen, können sie diese über die Identifikationsnummer der Urkunde oder des Fortbildungszertifikates im Portal www.kammerservice.de kontrollieren. Wurde ein entsprechendes echtes Dokument gefunden, wird dieses zum Vergleich mit den wichtigsten Daten angezeigt. Der TLfDI prüft den Verifikationsdienst noch, um die Sicherheit abschließend beurteilen zu können.

9.20 Health Care + Data Care: Datenschutz im MVZ

Im Berichtszeitraum trat ein Arzt eines MVZ (= Medizinisches Versorgungszentrum) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran und bat um datenschutzrechtliche Information über den Umgang mit Patientendaten in einem MVZ. Vor allem befürchtete der Arzt, sich nach § 203 Strafgesetzbuch (StGB) strafbar zu machen, wenn er die Daten seiner Patienten nicht schütze. Der TLfDI teilte dem besorgten Arzt zunächst mit, dass er für die Beurteilung von strafrechtlich relevanten Sachverhalten nicht zuständig sei. Aus datenschutzrechtlicher Sicht beriet der TLfDI den Arzt dahingehend, dass in aller Regel die Ärzte in einem MVZ die Patienten nicht gemeinsam, wie dies in einer Gemeinschaftspraxis der Fall ist, behandeln (vergleiche Beitrag 9.9 „Datenschutz in Berufausübungsgemeinschaften“). Nach der gesetzlichen Vorgabe des § 95 Abs. 1 SGB V sind Medizinische Versorgungszentren (MVZ) fachübergreifende, ärztlich geleitete Einrichtungen, in denen Ärzte, die in das Arztregister nach § 95 Abs. 2 Satz 3 Nr. 1 SGB V eingetragen sind, als Angestellte oder Vertragsärzte tätig sind. Häufig werden sogar ganze Arztpraxen in ein MVZ eingebracht. Grundsätzlich schließen die Patienten in einem MVZ nicht mit allen Ärzten einen gemeinschaftlichen Behandlungsvertrag.

Arztpraxen und MVZ sind in der Regel nicht-öffentliche Stellen (Wirtschaftsunternehmen), daher richtet sich die rechtliche Beurteilung der Datenverarbeitung nach dem Bundesdatenschutzgesetz (BDSG). Bei Patientendaten handelt es sich nach § 3 Abs. 9 BDSG um besondere Arten von personenbezogenen Daten, da sie Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig.

Was den gegenseitigen Zugriff auf die Patientendaten von den dem MVZ angeschlossenen Ärztinnen bzw. Ärzten anbelangt, so ist zumindest in den Fällen, in denen diese sich nicht wechselseitig vertreten, kein Grund dafür ersichtlich, dass jeder von ihnen auf die Daten aller Patientinnen und Patienten zugreifen kann. Je höher die Anzahl der Ärztinnen bzw. Ärzte und Fachrichtungen in einem MVZ ist, desto wichtiger wird die Frage nach einer Zugriffsdifferenzierung, d. h. nach einer internen technischen Beschränkung der Zugriffsmög-

lichkeiten auf die Patientendaten auf den jeweiligen behandelnden Arzt bzw. die Ärztin und die evtl. Vertretung. Teilweise wird von den Patientinnen oder Patienten vor Beginn der Behandlung in einem MVZ eine Einwilligung für die Möglichkeit der Kenntnisnahme ihrer Daten durch alle Ärztinnen bzw. Ärzte in dem MVZ, eingeholt. Meist wird dann auch die Behandlung außer in Notfällen abgelehnt, wenn die Patientin oder der Patient die Einwilligungserklärung nicht unterschreibt. Offensichtlich wird hier zumindest erkannt, dass ein Zugriff durch alle Ärztinnen bzw. Ärzte keineswegs selbstverständlich ist. Das Einholen einer Einwilligung in nicht erforderliche Zugriffsmöglichkeiten ist jedoch eine rechtlich problematische und nicht im Interesse der Patientinnen und Patienten liegende Verfahrensweise.

Wegen der in einem MVZ hohen Anzahl von angeschlossenen Ärzten mit teils auch unterschiedlichen Fachrichtungen, ist ohne eine Einwilligung der Patienten eine strikte Trennung der (elektronischen) Verwaltung der Behandlungsakten der jeweiligen Ärzte untereinander geboten. Die Patientendaten des MVZ sind in separaten Mandaten zu verarbeiten. Pauschale Übermittlungen oder Abrufe bzw. Einrichtung der Möglichkeit der Kenntnisnahme von Patientendaten der jeweils anderen Arztpraxis sind grundsätzlich nicht ohne Weiteres zulässig. Die Trennung ist auch für die Patienten deutlich erkennbar zu machen, um ihnen die Wahrnehmung ihrer Persönlichkeitsrechte gegenüber den jeweiligen Ärzten zu gewährleisten (räumliche Distanz, Firmierung bzw. optischer Auftritt). Nutzen die Praxis-Partner in einem MVZ ein gemeinsames EDV-System, so sollte dies ermöglichen, dass verschiedene Kennungen eingerichtet werden, die regelmäßig nur den Zugriff auf die Daten der „eigenen“ Patienten ermöglichen. Der Umstand, dass das MVZ-Personal in der Regel für alle Ärzte arbeitet und damit zumeist Zugriff auf alle Patientenakten und -dateien hat, schließt ein Zugriffsverbot für den nicht behandelnden Arzt rechtlich nicht aus. Im Rahmen der gegenseitigen Vertretung, die gegebenenfalls auch in einem MVZ oder bei einer Praxisgemeinschaft erfolgen kann, muss der Patient bei der Behandlung durch den Vertreter diesem die Einsichtnahme in die Behandlungsunterlagen gestatten.

Für eine Übermittlung zwischen den getrennten Einrichtungen bedarf es daher grundsätzlich einer Einwilligung des Patienten.

Arztpraxen und MVZ sind in der Regel nicht-öffentliche Stellen (Wirtschaftsunternehmen), daher richtet sich die rechtliche Beurteilung der Datenverarbeitung nach dem Bundesdatenschutzgesetz (BDSG). Bei Patientendaten handelt es sich nach § 3 Abs. 9 BDSG um besondere Arten von personenbezogenen Daten, da sie Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig.

Lehrerin zeigt Schülern etwas am Laptop – © contrastwerkstatt / Fotolia.com

10 Schule

10.1 Sammelbestellungen von Schultaschenrechnern – bezahlbar, aber unberechenbar?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr aus der Anfrage eines Journalisten von möglichen Datenschutzverstößen in mehreren Bundesländern im Zusammenhang mit dem Handel von Schultaschenrechnern. Auch in Thüringen warb ein Elektronikhändler bei den Schulen mit einer „Bequemeinzahlung“. Hierbei bestand zunächst die Befürchtung, dass Schulen bei der Anschaffung von Schülertaschenrechnern klassenweise Schülerdatensätze an diesen Händler übermitteln, möglicherweise ohne Wissen und Einwilligung der Eltern und Schüler. Nach der gegebenen Rechtslage hätten Schulen bzw. einzelne Klassenlehrerinnen und -lehrer nach § 57 Abs. 4 Nr. 3 Thüringer Schulgesetz an den Händler personenbezogene Daten von Schülern und Eltern nur aufgrund einer rechtswirksamen Einwilligung der Betroffenen übermitteln dürfen. Der TLfDI wandte sich zunächst umgehend an das damalige Thüringer Ministerium für Bildung, Wissenschaft und

Kultur, um dort die Staatlichen Schulämter entsprechend zu unterrichten. Gleichzeitig nahm der TLfDI Kontakt mit dem Thüringer Elektronikhändler auf, der den Schulen angeboten hatte, den schul- und klassenweisen Bestellvorgang von Schultaschenrechnern in eigener Regie zu übernehmen. Der Händler hatte sich in einer ersten Stellungnahme dahingehend geäußert, die Klassenlisten mit Vor- und Zunamen der Schüler ausschließlich für die Bestellabwicklung zu benötigen, nicht aber für andere Zwecke, etwa zur Werbeansprache zu nutzen. Der TLfDI führte daraufhin mit dem Unternehmen ein Gespräch zu der bestehenden Problematik. Im Ergebnis hat das Unternehmen ein Schreiben mit Hinweisen zum Datenschutz entworfen, in dem das Bestellverfahren den Schulen bzw. den Lehrern erläutert wurde und aufgeführt war, welche Schülerdaten zur Abwicklung von Sammelbestellungen benötigt werden. Insbesondere wird darin erklärt, dass die dorthin übermittelten Schülerdaten ausschließlich für die Abwicklung der Sammelbestellung verarbeitet werden und die Daten weder an Dritte übermittelt noch zu Werbezwecken verwendet wurden. Den Schulen wurde ausdrücklich empfohlen, vor einer Sammelbestellung der Schülertaschenrechner die schriftliche Zustimmung der Eltern für die Übermittlung des Schülernamens und in einigen Fällen auch der Klassenbezeichnung an das Unternehmen einzuholen. Denn letztlich sind die Schulen für die datenschutzgerechte Durchführung des Bestellverfahrens verantwortlich.

Die Schule bzw. die Lehrer tragen im Rahmen der schulgesetzlichen Bestimmungen die datenschutzrechtliche Verantwortung für die Zulässigkeit der Übermittlung von Schüler- und Elterndaten an Dritte. Die Angebote des Handels über Sammelbestellungen sind dahingehend von den Schulen zu prüfen. Die Übermittlung darf nur erfolgen, wenn eine rechtliche Vorschrift dies erlaubt oder wenn zuvor eine schriftliche Einwilligung bei den Eltern und ggf. auch Schülern eingeholt wurde.

10.2 Datenschutz bei Schulen in privater Trägerschaft

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit erreichen immer wieder allgemeine Anfragen von Bürgern, die wissen wollen, welche datenschutzrechtlichen Regelungen in Schulen gelten, die nicht in staatlicher, sondern in

privater Trägerschaft stehen. Hierzu ist festzustellen, dass in Thüringen auf Schulen in privater Trägerschaft als nicht-öffentliche Stellen das Bundesdatenschutzgesetz (BDSG) Anwendung findet. Der TLfDI ist für diese Stellen gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit § 38 Abs. 6 BDSG zuständige Aufsichtsbehörde für den Datenschutz. Der TLfDI kann bei diesen Stellen bei datenschutzrechtlichen Verstößen ein Ordnungswidrigkeitenverfahren einleiten und ein Bußgeld verhängen. Diese Möglichkeit steht ihm bei den staatlichen Schulen nicht zu. Weiterhin gilt für die Schulen in privater Trägerschaft das Thüringer Gesetz über Schulen in freier Trägerschaft. Dieses Gesetz enthält aber mit einer Ausnahme keine datenschutzrechtlich relevanten Regelungen. Diese Ausnahme betrifft die Anwendbarkeit der Bestimmungen über die Zusammenarbeit zwischen Schule und Jugendhilfe gemäß § 55 a Thüringer Schulgesetz. Bei der Bestellung eines Beauftragten für den Datenschutz finden die Bestimmungen der §§ 4 f, 4 g BDSG Anwendung. Die Schulen in privater Trägerschaft sind deshalb verpflichtet, einen Datenschutzbeauftragten einzusetzen, wenn mindestens 20 Beschäftigte der Schule mit der nicht automatisierten Datenverarbeitung oder mehr als neun Beschäftigte mit der automatisierten Datenverarbeitung beschäftigt sind oder wenn ein automatisiertes Verfahren betrieben wird, etwa eine Videoüberwachung, welche einer Vorabkontrolle unterliegt.
Als weitere Ausnahme sind die Schulen in kirchlicher Trägerschaft zu nennen. Hier kommen, je nachdem, ob ein evangelischer Träger oder ein katholischer Träger verantwortlich ist, die jeweiligen kirchlichen Datenschutzgesetze zur Anwendung. Der TLfDI hat hier keine Zuständigkeit.

Bei der Anwendung der datenschutzrechtlichen Bestimmungen ist die Trägerschaft der jeweiligen Schule zu berücksichtigen. Je nach rechtlicher Einordnung des Trägers gelten andere Bestimmungen. Bei den staatlichen Schulen sind dies insbesondere das Thüringer Schulgesetz (z. B. § 57 ThürSchulG), die Thüringer Schulordnung (z. B. § 136 ThürSchulO) und ergänzend das ThürDSG. Bei den Schulen in freier Trägerschaft sind dies das BDSG, vertragliche Regelungen der Schule und § 55 a ThürSchulG. Bei Schulen in kirchlicher Trägerschaft gelten bei einem evangelischen Träger das „Kirchengesetz über den Datenschutz der Evangelischen Kirche in

Deutschland“ und bei einem katholischen Träger die „Anordnung über den kirchlichen Datenschutz“.

10.3 Essen gegen Fingerabdruck

Aus der Presse erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass in einer Thüringer Region Unsicherheit herrschte, weil im Kantinenbereich einer Schule die Fingerabdrücke aller Schüler zum Zweck der Essensausgabe erfasst werden sollten. Diese Unsicherheit ist auch grundsätzlich berechtigt, gerade wenn es um unsere biometrischen Daten, wie zum Beispiel Fingerabdrücke geht. Warum? Hierfür gibt es verschiedene Gründe. Vor allem aber, weil man über diese Datensätze, je nachdem, wie sie gespeichert sind, eine Person für alle Ewigkeiten eindeutig identifizieren kann.
Der TLfDI kontrollierte daher umgehend das Unternehmen, welches das o. g .Verfahren durchführen wollte. Dabei wurde festgestellt, dass das Verfahren überhaupt noch nicht zum Einsatz kam. Da der TLfDI Unternehmen gegenüber auch eine Beratungsfunktion innehat, entwickelte sich aus der begonnenen Kontrolle eine datenschutzrechtliche Beratung, um dem Unternehmen aufzuzeigen, welche gesetzlichen Grenzen zu beachten sind und welche Voraussetzungen ein solches System erfüllen muss, um überhaupt zulässig zu sein. Unmöglich ist dies nämlich auch im Rahmen des Bundesdatenschutzgesetzes nicht.
Dort ist geregelt, dass das Erheben und Verarbeiten von personenbezogenen Daten nur zulässig ist, wenn das Bundesdatenschutzgesetz (BDSG) oder eine andere Vorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt, § 4 Abs. 1 BDSG.
Eine Norm, die das Erfassen und Speichern von Fingerabdrücken durch private Unternehmen erlaubt, ist nicht existent. Zwar kann ein Unternehmer nach dem BDSG (unter anderem) alle Daten erheben und verarbeiten, die er für die Begründung, Durchführung oder Beendigung eines Rechtsgeschäfts benötigt, jedoch ist er hier an eine Erforderlichkeitsprüfung gebunden, § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Zwar wird der Umfang der Erforderlichkeit durch das eigentliche Rechtsgeschäft bestimmt, jedoch lässt sich ein Fingerabdruck, der zum Zweck der Identifikation genutzt wird, immer durch etwas weniger in die Rechte des Betroffenen Eingreifendes ersetzen. Durch eine Chipkarte zum Beispiel, die ausgelesen wird.

Daher ist das Erheben von Fingerabdrücken und deren weitere Verarbeitung nur mit einer entsprechenden wirksamen Einwilligung des Betroffenen möglich. Diese muss vor allem freiwillig sein. Im Falle der Essensausgabe der Schulkantine bedeutet dies, dass der Anbieter auch Alternativen zum Bezahlen mit Fingerabdruck anbieten muss. So zum Beispiel die Barzahlung oder das Bezahlen per Chipkarte. Darüber hinaus muss der Fingerabdruck auf eine Art erkannt werden, die sicherstellt, dass aus dem abgespeicherten Wert der eigentliche Fingerabdruck nicht wieder errechnet werden kann.
Dies wird so erreicht, dass aus bestimmten Punkten im Fingerabdruck ein Zahlenwert errechnet wird. Dieser wiederum ist der Person dann zugeordnet. Die Berechnungsmethode wird so gewählt, dass eine Rückrechnung, also ein Erstellen des Fingerabdrucks aus dem Zahlenwert, nicht möglich ist. Diese Vorgehensweise ist auch dann notwendig, wenn per Einwilligung gearbeitet wird, da auch dann die Verpflichtung zu notwendigen technisch-organisatorischen Maßnahmen nach § 9 BDSG besteht.
Im Rahmen der Beratung wurden dem Unternehmen zunächst die Voraussetzungen für ein legales Betreiben des angestrebten Verfahrens vermittelt. Sodann wurde darauf hingewirkt, dass alle notwendigen Maßnahmen, die das BDSG vorschreibt, veranlasst werden. Nach Abschluss dieser Beratung durch den TLfDI hat das Unternehmen alle notwendigen Maßnahmen umgesetzt. Das Verfahren kann jetzt im vom BDSG vorgeschriebenen Rahmen durchgeführt werden. Insbesondere hat das Unternehmen eine Einwilligung entworfen, die die Betroffenen in ausreichender Weise über das Verfahren informiert und gleichzeitig Alternativen aufzeigt, für den Fall, dass nicht eingewilligt wird.

Manche Verfahren sind nicht ohne Einwilligung der Betroffenen durchzuführen. Dabei ist insbesondere darauf zu achten, dass die Betroffenen ausreichend informiert sind, das Schriftformerfordernis eingehalten und darauf hingewiesen wird, was die Folgen einer Verweigerung der Einwilligung sind. Der TLfDI hat Unternehmen und ihren betrieblichen Datenschutzbeauftragten (bDSB) gegenüber auch eine Beratungspflicht, die gerne jederzeit, aber insbesondere dann, wenn Sie unsicher sind, in Anspruch genommen werden kann.

Close-up image of a firm handshake between two colleagues – © Saklakova / Fotolia.com

11 Unternehmensverkauf

11.1 Hotelübernahme = Datenübernahme?

Bei Unternehmenstransaktionen wird den Interessenten üblicherweise schon im Vorfeld eine Vielzahl von Informationen zur Verfügung gestellt. Dadurch wird es überhaupt erst möglich, das Kaufobjekt wirtschaftlich und rechtlich zu beurteilen. Selbstverständlich spielen dabei auch eine Menge personenbezogener Daten wie etwa Mitarbeiter-, Lieferanten- und Kundendaten eine gewichtige Rolle.
Auch in diesem Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage eines ehemaligen Hotelbetreibers, inwieweit die vorhandenen Kundendaten, insbesondere die auf den PCs, von dem neuen Pächter des Hotels, einem neuen Unternehmen, weiter genutzt werden dürften. Dem TLfDI wurde mitgeteilt, dass das Hotel als Unternehmergesellschaft firmiert und es wegen anderweitiger Streitigkeiten einen Insolvenzantrag gestellt habe. Im Rahmen dieses Insolvenzantrages wurde das Hotel von einem anderen Pächter übernommen, der es als Einzelunternehmer weiterführte. Dabei sind sämtli-

che Unterlagen wie auch PCs samt Daten in den Besitz des neuen Pächters übergegangen. Neben sonstigen Informationen befanden sich darunter sämtliche Kundendaten, ca. 6.000, des ehemaligen Hotelbetreibers sowie Kreditkarten- und Buchhaltungsdaten.
Insoweit fragte der ehemalige Hotelbetreiber als Gesellschafter bzw. möglicher ehemaliger Gesellschafter der Unternehmergesellschaft den TLfDI, ob eine solche Verfahrensweise rechtmäßig sei.
Der TLfDI teilte dem ehemaligen Hotelbesitzer mit, dass nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei der „Übertragung" von Kundendaten von einem Unternehmen auf das Nachfolgeunternehmen handelt es sich um eine Übermittlung, die wieder Teil der Datenverarbeitung ist. Der Aussage von § 4 Abs. 1 BDSG folgend benötigt die alte Unternehmergesellschaft bzw. der Insolvenzverwalter daher eine Erlaubnisnorm oder die Einwilligung der jeweiligen Kunden, um die Daten von sich auf das Nachfolgeunternehmen zu übertragen.
Als Rechtsgrundlage kommt hier allenfalls § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG in Betracht, da eine Weitergabe von Daten aufgrund einer Veräußerung des Unternehmens eine Zweckänderung zum bei Erhebung festgelegten Zweck darstellt. Immerhin sind die Daten damals zur Durchführung eines Beherbergungs- und Bewirtungsvertrages erhoben und gespeichert worden. § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG setzt allerdings zunächst ein berechtigtes Interesse eines Dritten voraus. Darüber hinaus wird noch verlangt, dass kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Bei gespeicherten Kundendaten besteht ein solcher Grund allenfalls dann nicht, wenn die Betroffenen jeweils vor Übermittlung an das neue Unternehmen über dieses informiert worden sind, ihnen eine Möglichkeit zum Widerspruch eingeräumt wurde und sie nicht widersprochen haben.
Der TLfDI benötigt für eine abschließende datenschutzrechtliche Beurteilung von dem ehemaligen Hotelbetreiber jedoch weitere Informationen. Im hiesigen Fall konnte der ehemalige Hotelbetreiber diese bisher nicht nachreichen. Das Verfahren ist noch nicht abgeschlossen.

Bei der „Übertragung“ von Kundendaten von einem Unternehmen auf das Nachfolgeunternehmen handelt es sich um eine Datenübermittlung als Teil der Datenverarbeitung i. S. d. § 4 Abs. 1 BDSG ist. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

11.2 Augen auf beim Unternehmenskauf!

Aufgrund einer Beschwerde brachte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfahrung, dass bei einem Unternehmensverkauf die personenbezogenen Daten der Kunden datenschutzrechtlich nicht richtig übermittelt wurden. Im Fall ging es konkret um den Abschluss von Mietverträgen zur Nutzung von Schulschließfächern zwischen dem Unternehmen und den Schülern, vertreten durch deren Eltern. In den Mietverträgen waren jeweils der Name der Betroffenen und die Anschrift, Telefonnummer, Telefaxnummer, E-Mail-Adresse und die Bankverbindung sowie die Angabe der Klassenummer enthalten. Der Bevollmächtige des Unternehmens teilte dem TLfDI mit, dass der gesamte Geschäftsbereich, somit auch die Schließfachanlagen, zusammen mit den entsprechenden Verträgen an ein anderes Unternehmen veräußert wurde. Insoweit sei das Nachfolgeunternehmen in den Mietvertrag mit den Schülern eingetreten.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten und Nutzen personenbezogener Daten nur zulässig, wenn dies vom BDSG oder durch eine andere Rechtsvorschrift erlaubt wurde oder der Betroffene eingewilligt hat. Die Übermittlung fällt unter den Begriff der Verarbeitung, § 3 Abs. 4 Satz 1 BDSG. Liegt also weder eine Erlaubnisnorm noch eine Einwilligung in die Übermittlung vor, folgt hieraus die Rechtswidrigkeit der Übermittlung der Kundendaten.
Als Rechtsgrundlage kam hier zunächst der § 28 Abs. 1 Nr. 2 BDSG in Betracht. Danach ist das Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Der TLfDI stellte aber fest, dass der § 28 Abs. 1 Nr. 2 BDSG für die vorgenannte

Übermittlung als Rechtsgrundlage nicht in Frage kam, da die von dem Unternehmen übermittelten Daten ursprünglich zu dem Zweck erhoben wurden, mit den Kunden ein Mietverhältnis zu begründen und durchzuführen. Die mit diesem Zweck erhobenen Daten waren im Rahmen von § 28 Abs. 1 Satz 1 BDSG auch nur für diesen Zweck verwendbar, § 28 Abs. 1 Satz 2 BDSG. Dem Übermitteln personenbezogener Daten im Rahmen eines Unternehmensverkaufs liegt jedoch ein anderer Zweck, nämlich der einer Erfüllung einer Verbindlichkeit gegenüber einem Dritten – dem Nachfolgeunternehmen – zugrunde.
Auch kam der TLfDI bei der Prüfung, ob hier der § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG als Erlaubnisnorm einschlägig war, zu keinem anderen Ergebnis. Danach ist die Übermittlung für einen anderen Zweck – also eine zweckfremde Übermittlung – unter den Voraussetzungen des Abs. 1 Satz 1 Nr. 2 oder 3 zulässig. Die Abwägung, die im Rahmen des § 28 Abs. 1 Nr. 2 BDSG zwischen den berechtigten Interessen des Unternehmens und den schutzwürdigen Interessen der Betroffenen zu treffen war, fiel hier nach Überprüfung der Sach- und Rechtslage durch den TLfDI nicht zugunsten des Unternehmens aus. Ein Überwiegen des Interesses des Unternehmens lag auch dahingehend nicht vor, weil das Unternehmen vor der Übermittlung nicht die einzelnen Betroffenen über den Verkauf informiert und ihnen die Gelegenheit zum Widerspruch gegen die Verwendung der personenbezogenen Daten eingeräumt hatte.
Schließlich war auch mangels vorheriger Informationen der Betroffen der § 28 Abs. 2 Nr. 2a BDSG nicht anwendbar. Danach ist die Übermittlung personenbezogener Daten für einen anderen Zweck zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist. Auch hier stellte der TLfDI fest, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Übermittlung hatten.
Im Ergebnis handelte es sich hier mangels Vorliegen einer einschlägigen Rechtsgrundlage und einer entsprechenden Einwilligung der Betroffenen um einen Verstoß gegen das BDSG. Zuständigkeitshalber hat der TLfDI aufgrund des Sitzes und der Niederlassung des Unternehmens in Baden-Württemberg das Verfahren an den Landesbeauftragten für den Datenschutz Baden-Württemberg abgegeben.

Wird ein Unternehmen verkauft, werden stets auch Daten übertragen. Ein rechtmäßiges Vorgehen setzt voraus, dass die Betroffenen – z. B. Mieter – angeschrieben und unter Hinweis auf das sich daraus ergebende außerordentliche Kündigungsrecht (§ 543 BGB bei Mietverträgen) über den geplanten Verkauf der Mietsache informiert werden und so die Möglichkeit erhalten, einer für diesen Zeitpunkt geplanten Datenübermittlung entweder entgegenzuwirken (Kündigung) oder in diese einzuwilligen.

11.3 Firmenverkauf, Akten inklusive

Es meldete sich ein Anrufer beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Anrufer hatte das Büro der insolventen X-GmbH samt Zubehör übernommen. Im Zuge der Sichtung der übernommenen Materialien stellte der Anrufer fest, dass dort auch mehrere Aktenordner mit Personalunterlagen sowie Rentenunterlagen enthalten sind. Bei diesen Akten handelt es sich um personenbezogene Arbeitnehmerdaten, für die die X-GmbH verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG) war. Der Insolvenzverwalter hatte mit dem Verbleib der Akten in dem ehemaligen Büro der X-GmbH im Zuge der Veräußerung personenbezogene Daten bekannt gegeben. Die Bekanntgabe von personenbezogenen Daten an einen Dritten stellt gemäß § 3 Abs. 4 Nr. 3a) BDSG eine Übermittlung dieser dar. Der TLfDI hat zunächst den Insolvenzverwalter ermittelt, der über das Vermögen der X-GmbH verfügte. Der Anrufer gab dem TLfDI seine Einwilligung dazu, die Telefonnummer dem bestellten Insolvenzverwalter der X-GmbH zu übergeben, um einen Termin für die Abholung der Akten zu vereinbaren. Daraufhin wurde der Insolvenzverwalter aufgefordert, innerhalb von 14 Tagen die unbefugt an Dritte übermittelten Personalakten in den ehemaligen Büroräumen der X-GmbH abzuholen und diese unter Berücksichtigung datenschutzrechtlicher Vorschriften aufzubewahren. Innerhalb von einer Woche meldete sich der Insolvenzverwalter und gab bekannt, dass die Akten aus dem ehemaligen Büro der X-GmbH geräumt und datenschutzkonform verwahrt wurden.

Auch im Insolvenzverfahren eines Unternehmens bleibt dieses im Hinblick auf Arbeitnehmerdaten verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes.

Autobahnstau 2014 – © Kara / Fotolia.com

12 Verkehr

12.1 Kameras auf Schiene

Videokameras polarisieren. Es gibt Teile in der Bevölkerung, die Videokameras super finden, meist, weil diese Menschen hierdurch ein falsches Gefühl der Sicherheit vermittelt bekommen, ein anderer Teil der Bevölkerung fühlt sich aber immer öfter beobachtet und lehnt diese Videoüberwachung ab. Die Wahrheit liegt, wie so oft, irgendwo in der Mitte. Videoüberwachung ist nicht per se verboten. Aber die Zulässigkeitsvoraussetzungen sind recht hoch aufgehängt.
Auch in Bus und Bahn hat die Videoüberwachung immer weiter zugenommen. Inzwischen ist ein Maß erreicht worden, dass die Nutzung von kommunalen oder regionalen öffentlichen Verkehrsmitteln vollkommen unmöglich macht, ohne sich in nahezu 100% videoüberwachte Bereiche zu begeben.
Dass dieser Zustand mit den vom Gesetzgeber geschaffenen Regelungen zur Videoüberwachung in diesen Bereichen nicht vereinbar ist, scheint niemanden mehr zu interessieren. Denn bereits 2001 haben sich die Aufsichtsbehörden für den Datenschutz und der Ver-

band Deutscher Verkehrsunternehmen zusammengesetzt und eine Orientierungshilfe zur Videoüberwachung im öffentlichen Nahverkehr erstellt.
Auch Gespräche der Aufsichtsbehörden mit Betreibern und ausschreibenden Stellen haben zur Erkenntnis geführt, dass eine Prüfung der Zulässigkeit solcher Videoüberwachung in der Realität quasi nicht mehr durchgeführt wird. Aus diesem Grund haben die Aufsichtsbehörden für den Datenschutz unter Mitarbeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine neue, vollkommen überarbeitete Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln erarbeitet, die den gesetzlichen Rahmen für den zulässigen Einsatz von Videotechnik in Bus und Bahn erläutert. (OH „Videoüberwachung in öffentlichen Verkehrsmitteln“ – siehe Anlage 9).
Unter dem Eindruck, dass Videoüberwachung von weiten Teilen der Bevölkerung in diesem Bereich gewollt ist, werden Bahnlinien zumindest bei Neuausschreibungen mit zwingend vorgeschriebener flächendeckender Videoüberwachung (ca. 95% des Zuges) ausgeschrieben. Prüft nun der Gewinner der Ausschreibung die Zulässigkeit der Videoüberwachung nach den Regeln des BDSG unter Berücksichtigung des Einzelfalls und kommt zum Schluss, dass einzelne oder gar die komplette Videoüberwachung des Zuges unzulässig ist, hat er die Wahl zwischen Pest und Cholera.
Entweder kann er gegen Ausschreibungskriterien verstoßen und so eine empfindliche Vertragsstrafe, Subventionsrücknahmen oder Ähnliches riskieren oder er betreibt die Videoüberwachung, wie gefordert, in der Hoffnung, kein empfindliches (bis zu 300.000 Euro) Bußgeld von der zuständigen Ordnungswidrigkeiten-Behörde auferlegt zu bekommen. Ist nämlich die Videoüberwachung rechtswidrig, werden die mit ihr erhobenen und gespeicherten Daten unbefugt erlangt, was einen Ordnungswidrigkeitentatbestand verwirklicht. Für Thüringen ist der TLfDI diese Bußgeldbehörde.
Um diese Zwangslage zumindest in Thüringen für die Zukunft zu vermeiden, hat der TLfDI Gespräche mit dem für solche Ausschreibungen zuständigen Ministerium geführt. Das Ergebnis dieser Gespräche ist zunächst positiv: Es wird geprüft, ob in Zukunft die Ausschreibungen die reine technische Möglichkeit einer Videoüberwachung fordern und den Einsatz selbst dem Betreiber überlassen. Dann kann dieser in eigener Hoheit darüber entscheiden, ob eine

Videoüberwachung eingesetzt wird oder nicht und diese gegebenenfalls auf das zulässige Maß beschränken.

Nur weil im Ausschreibungstext eine Videoüberwachung gefordert wird, ist diese noch nicht zulässig. Vielmehr muss sie sich an der allgemeinen Regelung des § 6b Bundesdatenschutzgesetz messen lassen. Diese Bestimmung verlangt eine Einzelfallentscheidung, weswegen für jede Kamera eine separate Prüfung durchgeführt werden muss. Daher kann am Ende als Ergebnis einer datenschutzrechtlichen Prüfung durchaus die Zulässigkeit aller, einzelner oder keiner Kameras in einem Zug vorkommen. Die Verantwortung für die Rechtmäßigkeit der Videoüberwachung trägt im Übrigen der Betreiber des Verkehrsmittels.

12.2 Das Auto ist ein mieser Verräter

Die moderne technische Automobilausstattung bringt es mit sich, dass – zumindest in neueren Fahrzeugen – umfassende Daten über Fahrverhalten und Fahrroute erhoben werden können. Möglich ist sogar, in Erfahrung zu bringen, wann der Fahrer geschaltet und mit welcher Intensität er wo gebremst hat. Bereits jetzt interessieren sich die Kfz-Versicherer für diese Daten und wollen ihre Versicherten dazu bringen, eine Black-Box einbauen zu lassen, die das Fahrverhalten ebenfalls beobachtet. Es ist auch nicht auszuschließen, dass derjenige, der in einen Unfall verwickelt ist, in gar nicht ferner Zukunft herangezogen werden wird, seine Fahrzeugdaten zu seiner Belastung auslesen zu lassen – ein Verstoß gegen das im Allgemeinen Persönlichkeits-Grundrecht wurzelnde Selbstbelastungsverbot! Als Gegenleistung soll dann zwar die Versicherungsprämie um etwa 5 % gesenkt werden –bei entsprechend negativem Fahrverhalten wird diese jedoch wieder erhöht werden. Ob hierin noch eine freiwillige Datenpreisgabe des Betroffenen gesehen werden kann, wird derzeit kontrovers diskutiert. Die Gefahren einer derartigen Profilbildung sowie das Wecken von Daten-Begehrlichkeiten liegen auf der Hand, so in einer Pressemitteilung „Das Auto – Black-Box außer Kontrolle“ des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) 2014 nachzulesen (Anlage 18). Auch der deutsche Verkehrsgerichtstag 2014 beschäftigte sich u. a. mit der Frage „Wem gehören die Fahrzeugdaten?“ und forderte klare

Regeln zum Austausch von Daten und Informationen aus dem Fahrzeug.
So bleibt derzeit z. B. unklar, welche Daten der Fahrzeugbesitzer einsehen kann, welche Daten Automobilhersteller und Service-Werkstätten und andere Verkehrsteil-nehmer auslesen können und dürfen und wie man bspw. als Besitzer eines Autos die Daten löschen kann. Diese Fragen sollte sich ein Besitzer eines Fahrzeuges – wenn er es nicht schon beim Kauf eines Fahrzeuges getan hat – spätestens beim Verkauf seines Autos stellen. Denn auch die Infotainment-Anwendungen, wie z. B. Navigation, Video, Audio, Radio, Telefon, Internet usw., speichern unter Umständen die Daten oder die Namen der aufgerufenen Video-/Audio-Dateien oder wer wann wen angerufen hat, bis hin zur kompletten auf dem Handy gespeicherten Kontaktliste.
Aber nicht nur der datenschutzrechtliche Umgang von gespeicherten Daten muss zukünftig geregelt werden.
Wie moderne Computer oder gar vernetzte Computer in Unternehmen und Behörden sind auch Fahrzeuge, die (partiell) computergesteuert sind, real von Hacker-Angriffen bedroht. So mögen das elektronische Türe-Knacken und der anschließende Autodiebstahl zwar auch ein strafrechtliches Delikt sein, aber es geht datenschutzrechtlich um viel mehr.
Aus Sicht des TLfDI können Hacker-Angriffe eines Tages auch irgendwann dazu führen, dass ganz konkret bestimmte Autos manipuliert oder ausspioniert werden, Daten verfälscht werden oder bewusst bspw. das Auto einem Unfall zugeführt wird und so Leib und Leben der Fahrzeuginsassen in Gefahr geraten. Es besteht sogar aufgrund der hochausgereiften Computertechnik irgendwann die Gefahr, dass bspw. gleichzeitig hunderte Autos zu einem gleichen Zeitpunkt per Hacker-Angriff manipuliert werden. So lässt sich dann bspw. eine ganze Stadt lahmlegen oder bei einem Terroranschlag werden zuvor sämtliche Autos von Hilfs- und Rettungseinheiten destabilisiert.
IT-Sicherheit und Datenschutz müssen also dringend auch in der Automobilbranche Einzug halten. Hierzu bedarf es herstellerübergreifend entsprechend festgelegter Standards, Lösungen und Maßnahmen, um die IT-Sicherheit und den Datenschutz sicherzustellen. Cyber-Sicherheit macht nicht vor dem Auto halt, im Gegenteil. Durch die Vernetzungsmöglichkeit der Auto-Computer ergibt sich

nunmehr eine neue Angriffsfläche, auch hinsichtlich der an das Auto anschließbaren Geräte.
Der TLfDI teilte deshalb bereits 2014 mit, dass er sich dafür einsetzen wird, dass der Bundesgesetzgeber sich der Thematik annimmt. Zudem wies der TLfDI im Rahmen eines Vortrags an der Juristischen Fakultät der Universität Augsburg im Oktober 2015 bei der Tagung „Autorecht 2015 – autonomes Fahren“ noch einmal auf die rechtlichen Probleme der Datenerfassung, Weiterleitung und Verarbeitung diesbezüglicher Daten hin.

Datenschutz und IT-Sicherheit müssen auch für die in Autos verbauten Geräte gelten.
Hierzu bedarf es herstellerübergreifend entsprechend festgelegter Maßnahmen, um die IT-Sicherheit, den Datenschutz sicherzustellen. Der TLfDI wird sich dafür einsetzen, dass der Bundesgesetzgeber sich der Thematik annimmt, damit für die Autofahrer in Deutschland die Rechtssicherheit wiederhergestellt wird.

Stempel 2 Datenschutz – © S. Engels / Fotolia.com

13 Ordnungswidrigkeiten

13.1 Die Ordnungswidrigkeitenverfahren nehmen zu.

Wie bereits im letzten Tätigkeitsbericht dargestellt, ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seit Übertragung der Zuständigkeit für den Datenschutz im

nicht-öffentlichen Bereich auch zuständige Behörde für Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG) geworden. Das Ordnungswidrigkeitenverfahren ist eine besondere Unterart des Verwaltungsverfahrens. Es ist streng von anderen Verfahren zu trennen. Im Unterschied zum grundsätzlich formfreien Verwaltungsverfahren handelt es sich um ein streng formalisiertes Verfahren mit vielen Parallelen zum strafrechtlichen Ermittlungsverfahren. Ziel des Verfahrens ist es, Verstöße gegen das Bundesdatenschutzgesetz zu ahnden und auf diesem Wege eine Änderung im Verhalten des Verstoßenden zu erreichen. Im Wesentlichen teilt sich die Befugnis des TLfDI in Ordnungswidrigkeiten wegen eines Verstoßes gegen Formalien des BDSG sowie gegen inhaltliche Verstöße auf. Erstere können mit einem Bußgeld bis zu 50.000 Euro, Letztere bis zu 300.000 Euro geahndet werden. Dabei wird die Höhe der Geldbuße durch die Bedeutung der Ordnungswidrigkeit und den Vorwurf, der den Täter trifft, bestimmt, aber bis zu einem gewissen Maße auch durch die finanzielle Leistungsfähigkeit des Täters. An die eben genannten Obergrenzen ist der TLfDI allerdings dann nicht gebunden, wenn der zu ahndende Verstoß einen finanziellen Vorteil erwirtschaftet hat, der über diese Obergrenzen hinausgeht. Dieser Vorteil kann dann ebenfalls abgeschöpft werden. Rechtswidriges Verhalten soll sich ja nicht lohnen.

Während im letzten Berichtszeitraum noch an der grundlegenden Integration des Bußgeldverfahrens in den Arbeitsablauf gearbeitet wurde, konnten die Abläufe in diesem Berichtszeitraum an mehreren Stellen verbessert werden, um die Effizienz der Verfahrensbearbeitung zu erhöhen. Nur so war es möglich, die immer weiter steigenden Fallzahlen zu bearbeiten.

Dies zeigt sich auch in einer Steigerung der beim TLfDI bearbeiteten Bußgeldverfahren um mehr als das Doppelte. Es wurden Geldbußen in Höhe von insgesamt knapp über 13.000 Euro verhängt.

Es ist allerdings davon auszugehen, dass die Fallzahlen weiter steigen werden. Dieser Anstieg kann dann mit Verfahrensverbesserungen kaum mehr abgefangen werden.

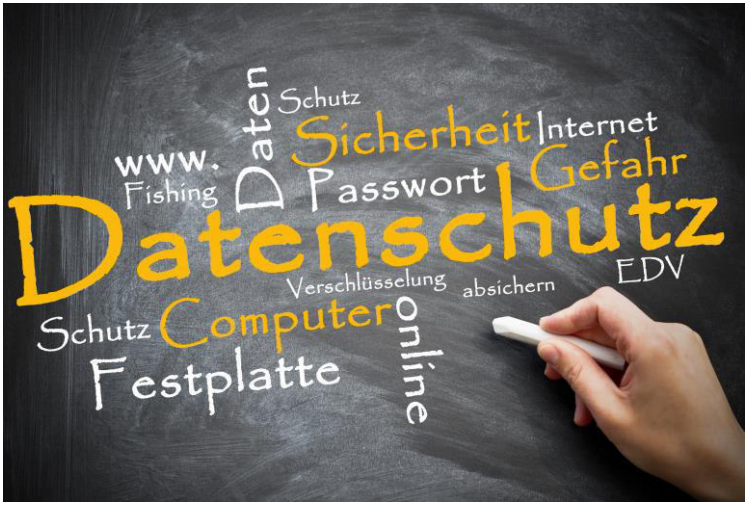
Im Wesentlichen verfolgte der TLfDI bei den formellen Verstößen gegen das BDSG die nicht oder nicht rechtzeitige Auskunftserteilung durch verantwortliche Stellen gegenüber dem TLfDI nach § 43 Abs. 1 Nr. 10 BDSG sowie die nicht oder nicht rechtzeitig erfolgte Auskunftserteilung durch verantwortliche Stellen gegenüber einzelnen Betroffenen im Rahmen deren Auskunftsrechts nach

§ 34 Abs. 1 BDSG. Dies ist besonders bedauerlich, da es sich um Verstöße handelt, die einfach zu vermeiden sind.

Bei den materiellen Verstößen handelt es sich meist um ein unbefugtes Erheben oder Verarbeiten von personenbezogenen Daten nach § 43 Abs. 2 Nr. 2 BDSG.

Wird eine vorsätzliche Handlung, die nach § 43 Abs. 2 BDSG eine Ordnungswidrigkeit darstellt, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen, handelt es sich um eine Straftat. Diese zu verfolgen, ist der TLfDI nicht befugt. Vielmehr verfolgt die jeweils zuständige Staatsanwaltschaft die Tat auf Antrag. Neben dem Opfer und der verantwortlichen Stelle selbst, sind die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und auch der TLfDI in solchen Fällen antragsberechtigt.
Hiervon hat er im Berichtszeitraum zweimal Gebrauch gemacht.

Das Bußgeldverfahren beim TLfDI nimmt immer weiter Fahrt auf. Die Verfahrenszahlen steigen und es besteht die konkrete Gefahr, dass nicht mehr alle Verfahren zügig bearbeitet werden können.



Datenschutz – © Marco2811 / Fotolia.com

14 Technischer und Organisatorischer Datenschutz

14.1 Happy Birthday – die elektronische Gesundheitskarte wird 10 Jahre alt

Bereits im November 2003 wurde das „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung“ (GKV-Modernisierungsgesetz – GMG) erlassen. Dies hatte zur Folge, dass auch das Sozialgesetzbuch (SGB) Fünftes Buch (V) u. a. in § 291 und § 291a geändert wurde. So wurde damals festgelegt, dass die Krankenversichertenkarte bis spätestens zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte zu erweitern ist. Auch wurde festgelegt, welche Daten die elektronische Gesundheitskarte beinhalten muss und welche Daten wie verarbeitet werden sollen.
Der Thüringer Landesbeauftragte für den Datenschutz berichtete in seinen Tätigkeitsberichten mehrfach darüber.
Allerdings ist die elektronische Gesundheitskarte erst seit dem 1. Januar 2015 Pflicht und gilt seit diesem Zeitpunkt bundesweit ausschließlich als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkassen beim Arzt oder Zahnarzt. Der Thüringer Landesbeauftragte für den Datenschutz und

die Informationsfreiheit (TLfDI) informierte daraufhin zum aktuellen Sachstand in einer Pressemitteilung (siehe Anlage 20). Seit dem 29. Dezember 2015 ist nun auch das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze in Kraft (E-Health-Gesetz). So soll nun mittels der elektronischen Gesundheitskarte die Verbesserung der Wirtschaftlichkeit, Qualität und Transparenz der Behandlung durch moderne Anwendungen und Informations- und Kommunikationstechnologien erzielt werden (siehe Beitrag 14.2 E-Health-Gesetz).
Damit auch die kommenden Anwendungen in Thüringen datenschutzrechtskonform umgesetzt werden, hat der TLfDI seine Gesprächsbereitschaft gegenüber der Landesärztekammer Thüringen und der Landesapothekerkammer Thüringen bekundet (siehe Anlage 14).
Unabhängig davon wird der TLfDI den weiteren Werdegang dieser Karte aufmerksam verfolgen.

Der Einsatz der elektronischen Gesundheitskarte wird auch künftig vom TLfDI kritisch beobachtet. Der TLfDI bittet daher um Hinweise, falls datenschutzrechtliche Probleme auftauchen.

14.2 E-Health-Gesetz des Bundes

„Health“ bedeutet Gesundheit. Verwirrend scheint, dass manchmal von eHealth und dann wieder von mHealth zu lesen ist. Wenn der Begriff mHealth benutzt wird, ist man im Bereich der „mobilen Gesundheit“, der Gesundheits-Apps, die Ihnen oder/und auch medizinischem Fachpersonal versprechen, durch die Anwendung auf Laptops, Smartphones oder nun beispielsweise digitalen Uhren Ihre Gesundheit verbessern zu können (siehe dazu 11. Tätigkeitsbericht Beitrag 11.8 mEalth). Der Begriff eHealth bedeutet „elektronische Gesundheit“ und umfasst die aktive Nutzung der Gesundheitskarte (siehe Beitrag 14.1) und die Telematik im Gesundheitsbereich, also generell die Nutzung von Informationstechnik innerhalb des Gesundheitswesens.
Seit 29. Dezember 2015 ist nun das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze (sog. E-Health-Gesetz) in Kraft. Per Gesetz soll mittels der elektronischen Gesundheitskarte die Verbesserung der Wirtschaftlichkeit, Qualität und Transparenz der Behand-

lung durch moderne Anwendungen und Informations- und Kommunikationstechnologien erzielt werden. Ziel dabei ist es unter anderem, die Einführung der elektronischen Gesundheitskarte einschließlich ihrer nutzbringenden Anwendungen zu unterstützen und die Telematik und die Interoperabilität der informationstechnischen Systeme im Gesundheitswesen zu verbessern. Unter Interoperabilität versteht man, dass Geräte oder Anwendungen (Software) so gestaltet werden, also so standardisiert werden, dass sie mit anderen Geräten oder Systemen zusammenarbeiten können. Auch würde sich dadurch der Patienten-Nutzen erhöhen, da eine zielgenauere und schnellere Behandlung möglich wäre und auch gefährliche Wechselwirkungen, z. B. durch das Erfassen von verordneten Medikamenten, verringert werden könnten.
Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte bereits im März 2015 in ihrer entsprechenden Entschließung Nachbesserungen zum Gesetzesentwurf (siehe Anlage 14). So mahnte sie insbesondere an, die Vertraulichkeit der Daten und Transparenz der Datenverarbeitung zu regeln. Da die Betroffenen selbst über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte entscheiden können, bedarf es eben der Transparenz, welche Daten durch wen verarbeitet werden können. Außerdem muss zu jeder Zeit die gebotene Vertraulichkeit der Daten gewährleistet sein. Auch im Hinblick darauf, dass insbesondere durch immer modernere Informationstechnik die Einschaltung externer Dienstleister durch Berufsgeheimnisträger nicht ausbleiben wird, bedarf es neben der technischen Sicherstellung der Vertraulichkeit weiterer Regelungen. Um nicht in die Gefahr eines Verstoßes gegen die Schweigepflicht (§ 203 StGB) zu kommen, gilt es, klare Rahmenbedingungen zu schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger überhaupt externe Dienstleister einschalten dürfen.

Bei der Verarbeitung personenbezogener Daten im Gesundheitswesen, spielen die Vertraulichkeit der Daten und die Transparenz der Datenverarbeitung eine wichtige Rolle. Um nicht in die Gefahr eines Verstoßes gegen die ärztliche Schweigepflicht zu kommen, gilt es auch, klare Rahmenbedingungen zu schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen.

14.3 Ein Schritt vor, zwei zurück – ist die Verschlüsselung politisch wirklich gewollt?

Durch die zunehmende digitale Vernetzung und die Erkenntnis, dass Sicherheitsbehörden heimlich Daten abgreifen und die Wirtschaftsspionage zunimmt, gewinnt die Verschlüsselung von Daten bei der Datenübermittlung und -speicherung verstärkt an Bedeutung.
Das Sicherheitsbedürfnis, dass nur Befugte Daten zur Kenntnis nehmen sollen, haben Bürger, Unternehmen und auch die öffentliche Verwaltung. Insbesondere Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie z. B. Ärzte, Anwälte, Psychologen und Steuerberater, müssen die Vertraulichkeit der Daten gewährleisten. Aber auch Journalisten und Abgeordnete haben großes Interesse daran, dass sich jedermann vertraulich an sie wenden kann.
Wie wichtig eine zuverlässige und sichere Verschlüsselung von Daten ist, hatte auch die Bundesregierung im Dokument „Digitale Agenda 2014–2017“ deutlich gemacht.

So heißt es in der Agenda:

> „Ohne Vertrauen in die Sicherheit und Integrität der digitalen Welt wird es nicht gelingen, die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen. Das Vertrauen zu stärken heißt daher zum einen, die Kommunikation über digitale Netze zu schützen und dafür den Zugang zu sicheren und einfach zu nutzenden Verschlüsselungsverfahren zu fördern.
> Zum anderen bedeutet es, dass wir unsere kritischen Infrastrukturen schützen. Wir wollen mit der Digitalen Agenda einen wesentlichen Beitrag dazu leisten, dass unser Land einer der sichersten digitalen Standorte weltweit bleibt.“

> „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungs-Standort Nr. 1 auf der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden.“

> „Wir fördern und fordern den Einsatz von vertrauenswürdigen IT-Sicherheitstechnologien, insbesondere von mehr und

besserer Verschlüsselung in der elektronischen Kommunikation."

Das war allerdings im August 2014.

Im Zusammenhang mit dem Anschlag in Paris am 7. Januar 2015 wurde dann sofort seitens der Politik über die Notwendigkeit einer Schwächung von Verschlüsselungstechnologien diskutiert, um so dem Terrorismus wirksam zu begegnen.

So konnte man schon im gleichen Monat einer Meldung bei www.heise.de entnehmen, dass – neben dem britischen Premier David Cameron und US-Präsident Obama – auch der Bundesinnenminister Thomas de Maizière nun Zugang zu verschlüsselten Daten wünscht. So forderte er, dass deutsche Sicherheitsbehörden befugt und in die Lage versetzt werden müssen, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen, wenn dies für ihre Arbeit und zum Schutz der Bevölkerung notwendig ist.

Aus diesem Grund wandte sich im März 2015 die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer ihrer Entschließungen an die Politik und forderte sie auf, sich aktiv für das Brief- , Post- und Fernmeldegeheimnis und bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptografischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich (siehe Anlage 15).

Kryptographische Verfahren dienen der Gewährleistung der Vertraulichkeit und Integrität. Insbesondere ist eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeit Dritter bereitzustellen. Kryptographische Verfahren durch staatliche Regulierungen zu un-

terbinden würde unter Umständen auch dem Brief-, Post- und Fernmeldegeheimnis entgegenwirken.

14.4 Löschung von Google-Suchergebnissen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit erreichen immer wieder telefonische Anfragen zu Internet-Suchmaschinen. Das Internet vergisst nie. So sind eingestellte Informationen im Internet über Jahre abrufbar, werden oft sogar weiter kopiert und woanders erneut sichtbar gemacht. Um Informationen im Internet zu finden, bedient man sich so genannter Suchmaschinen, als Beispiel sei hier die Suchmaschine von Google Inc. genannt. Welches Suchergebnis Suchmaschinen im Internet bei der Suche nach einem Begriff oder Namen anzeigen, bestimmt sich dabei in der Regel nach den kommerziellen Interessen der Suchmaschinenbetreiber und ihrer Vertragspartner.
Nun gibt es Fälle, in denen man nicht – oder nicht mehr – möchte, dass bestimmte Informationen über einen selbst auffindbar sind. Diese Informationen lassen sich allerdings nur löschen, wenn man sich direkt an den Betreiber der jeweiligen Website wendet, wo diese Informationen eingestellt sind. Ein Löschantrag über den Provider der Webseite ist in der Regel wenig erfolgreich. Oft bleiben beide Wege erfolglos, u. a. weil der Ansprechpartner seinen Sitz nicht in Deutschland bzw. im Europäischen Raum hat. Also lag die Idee nahe, wenn man schon nicht die Quellen löschen kann, dann wenigstens auf das Ergebnis von Suchmaschinen Einfluss zu nehmen.
So hatte der Europäische Gerichtshof am 13. Mai 2014 (C-131/12) Google Inc. dazu verpflichtet, auf Antrag bestimmte Suchergebnisse (Links) aus seinen Suchergebnislisten zu entfernen. Dies allerdings nur, wenn ein begründeter Widerspruch vorliegt und die Datenschutzrechte der betreffenden Person schwerer wiegen als das Interesse an der Verfügbarkeit der betreffenden Suchergebnisse.
Zudem darf der Europäische Gerichtshof nur Recht für die Europäische Union aussprechen. Die gleiche Suche mit Google – bspw. in den USA gestartet – zeigt weiterhin alle Treffer an.
So hat die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 in ihrer Entschließung „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ auch darauf hingewiesen, dass aufgrund der territorialen Unbeschränktheit des Internets, auch der Schutz des Einzelnen universell

gelten muss (siehe Link https://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/dsk_google_suchergebnisse.pdf).

Dies bedeutet, eine Beschränkung nur auf den Europäischen Raum ist für die Betroffenen derzeit nicht in jedem Fall zielführend.

Sollte man dennoch einen Antrag auf Entfernung von Suchergebnissen bei Google Inc. stellen wollen, muss man zunächst das begründete Löschbegehren direkt an Google Inc. richten. Dieses Antragsformular ist zu finden unter:
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de

Nach Antragstellung wird dann u. a. die Identität geprüft. Dies bedeutet, Google Inc. möchte einen Nachweis der Identität. Aus datenschutzrechtlicher Sicht sollten hierfür keine Kopien vom Personalausweis oder Reisepass verwendet werden! Man kann bspw. den Bibliotheksausweis oder andere Dokumente verwenden. Zudem empfiehlt es sich, generell zuvor auf der Kopie des zu sendenden Dokumentes alle Angaben (Zahlen), die nicht unmittelbar mit der Person zu tun haben, zu schwärzen.

Wird der hinreichend begründete Löschantrag von Google Inc. abgelehnt, kann man sich danach an die zuständige Aufsichtsbehörde, den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, wenden. Neben der Nennung des Suchbegriffes, des konkret zu löschenden Links und der geführten Kommunikation mit Google Inc. ist auch dessen vergebene Bearbeitungsnummer (Ticketnummer) mit zu übersenden.

Anträge auf Entfernen von Suchergebnissen bei Google sind direkt an Google Inc. zu stellen. Ein Antrag hat nur Erfolg, wenn eine gewisse Schwere der Persönlichkeitsrechtsbeeinträchtigung nachvollziehbar vorliegt. Bei der notwendigen Kopie eines identifizierenden Dokumentes sollte keine Kopie vom Personalausweis oder Reisepass verwendet werden, besser ist bspw. der Bibliotheksausweis.

Die Entfernung von Ergebnissen bei einer Suchmaschine bedeutet nicht, dass die eigentlichen Daten gelöscht wurden.

14.5 IT-Sicherheitsgesetz nicht ohne Datenschutz!

Seit den Terroranschlägen vom 11. September 2001 sind neben der Informationstechnik auch „kritische Infrastrukturen“ in den Mittelpunkt staatlicher Sicherheitsvorsorge gerückt. Im Jahr 2009 veröffentlichte das Bundesinnenministerium die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie).
Im Jahr 2011 folgte die „Cyber-Sicherheitsstrategie für Deutschland“, in der die Bundesregierung darauf hinwies, dass u. a. die Verfügbarkeit des Cyber-Raums die existenzielle Frage des 21. Jahrhunderts geworden sei. Wirtschaft und Bevölkerung seien auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen. Der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum könnten nach Angaben der Bundesregierung zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen.
Ein nationales Cyber-Abwehrzentrum wurde geschaffen, mit dem Ziel, die operative Zusammenarbeit der relevanten staatlichen Stellen zu optimieren und die Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle zu koordinieren.
Anfang 2013 wurde dann vom Bundesministerium des Innern ein Referentenentwurf eines IT-Sicherheitsgesetzes zur Diskussion veröffentlicht, welcher eine Reihe von Kritik erfuhr.
Anfang Januar 2015 ereignete sich das Attentat auf die Redaktion von „Charlie Hebdo“ in Paris. Mit dem Attentat begann nun auch wieder eine verschärfte politische Diskussion zur Sicherheit Deutschlands.
Ende Februar 2015 brachte die Bundesregierung dann den Gesetzentwurf für ein IT-Sicherheitsgesetz ein, um die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern.
Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die ausdrücklich die Notwendigkeit von Informationssicherheit befürwortet, kritisierte in ihrem entsprechenden Entschluss im März 2015 diesen Gesetzentwurf sehr scharf (siehe

https://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen2/entschliessungen89dsk/datenschutz_nach____charlie_hebdo___1.pdf). So seien beispielsweise die neuen Melde- und Benachrichtigungspflichten von erheblichen IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht mit einer datenschutzrechtlichen Meldepflicht von Datenpannen an die Datenschutzaufsichtsbehörden verbunden. Weiterhin kritisierte die Konferenz, dass zu unklar sei, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welchen Zweck erhoben, verarbeitet und gespeichert werden dürfen.

Wie der Zufall es so wollte: Während der Bundestag über dieses Gesetz diskutierte und es dann auch verabschiedete, ereilte das Bundestagsnetzwerk selbst ein Cyberangriff. Das IT-Sicherheitsgesetz trat, nun fast logisch, dann am 25. Juli 2015 in Kraft (Bundesgesetzblatt Teil 1 Nr. 31 vom 24. Juli 2015). Es schreibt die Einhaltung eines Mindestniveaus an IT-Sicherheit und Meldepflichten der Betreiber so genannter kritischer Infrastrukturen vor. Als kritische Infrastrukturen werden dabei gesehen: Einrichtungen, Anlagen oder Teile, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und zugleich von hoher Bedeutung für das funktionierende Gemeinwesen sind. Nach Angaben des Gesetzes sollen Einzelheiten zum Anwendungsbereich und zum Adresskreis noch in einer Rechtsverordnung bestimmt werden.

Mit dem IT-Sicherheitsgesetz wurde auch das Telekommunikationsgesetz geändert und die rechtliche Möglichkeit geschaffen, dass Telekommunikationsdiensteanbieter die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer bei Erforderlichkeit erheben und verwenden dürfen, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

Interessanterweise erfolgte, um ein paar Monate zeitversetzt, das parlamentarische Gesetzgebungsverfahren zum „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“, welches im Oktober 2015 vom Bundestag bestätigt wurde. Man erkennt unweigerlich, dass der Bedarf, die Informationstechnik zu schützen und insbesondere Terroristen zu überwachen,

offenbar zunimmt. Dies darf aber immer nur in ausgewogener Balance zum Datenschutz erfolgen. Die Datenschutzbeauftragten werden daher auch weiter darum kämpfen, dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren. Die Datenschutzbeauftragten werden daher weiter darum kämpfen, dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

14.6 eIDAS – was ist das?

Mit der Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates der Europäischen Union wurden Regelungen zur elektronischen Signatur für die Mitgliedstaaten getroffen. So regelte nachfolgend das deutsche Signaturgesetz (SigG) die Unterschiede und den Einsatz der elektronischen Signatur, der fortgeschrittenen elektronischen Signatur und der qualifizierten elektronischen Signatur. Einige nationale Normen schreiben zudem die qualifizierte elektronische Signatur vor, wenn die eigenhändige Unterschrift durch eine elektronische Unterschrift im elektronischen Dokument ersetzt werden kann. Um den Bürgern dies zu ermöglichen, sah man auch bereits beim elektronischen Personalausweis einen festen Speicherplatz für die qualifizierte elektronische Signatur vor. So kann man auf dem elektronischen Personalausweis eine qualifizierte elektronische Signatur speichern, um mit dem Personalausweis selbst elektronische Dokumente rechtsverbindlich und fälschungssicher elektronisch zu unterschreiben. Allerdings muss es tatsächlich eine qualifizierte elektronische Signatur sein. Dies bedeutet, ein Zertifizierungsdiensteanbieter hat die Identität des Eigentümers der elektronischen Signatur eindeutig überprüft und dies mittels eines elektronischen Zertifikates belegt. Mithilfe des Zertifikates kann dann festgestellt

werden, welcher Person die elektronische Signatur tatsächlich gehört.
Mit der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt vom 8. Juli 2009 wurden alle Mitgliedstaaten zudem verpflichtet, sicherzustellen, dass auch alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch abgewickelt werden können.
Dies bedeutete, auch in anderen Mitgliedstaaten ausgestellte elektronische Signaturen – hierbei insbesondere die qualifizierten elektronische Signaturen – zu prüfen und anzuerkennen.
Da aber europaweit diesbezüglich keine einheitlichen Regelungen vorhanden waren, wurde am 23. Juli 2014 die EU- „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ verabschiedet. Diese Verordnung wird auch als eIDAS-Verordnung bezeichnet (**e**lectronic **id**entification **a**nd trust **s**ervices). Entsprechend dem Erwägungsgrund 3 dieser Verordnung hatte zwar die damalige EU-Richtlinie 1999/93EG Regelungen zu elektronischen Signaturen festgelegt. Dies war jedoch geschehen, ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die eIDAS-Verordnung soll nun die Rechtsvorschrift jener Richtlinie stärken und erweitern.
Diese Verordnung (EU Nr. 910/2014) ist also ein weiterer Baustein, um die Nutzung grenzüberschreitender digitaler Dienste, die sichere elektronische Identifizierung und Authentifizierung und die Förderung des digitalen Binnenmarktes voranzutreiben. Sie gilt mit wenigen Ausnahmen ab dem 1. Juli 2016.
Inhaltlich unterscheidet sich die Verordnung zum Teil vom derzeit noch gültigen Signaturgesetz (SigG). Als Beispiel sei hier die elektronische Fernsignierung genannt: § 5 Abs. 6 i. V. m. § 17 Abs. 1 SigG sieht vor, dass bei der Erzeugung der qualifizierten elektronischen Signatur eine sichere Signaturerstellungseinheit einzusetzen ist und der Antragsteller auch solch eine Einheit besitzen muss. Die EU-Verordnung sieht nun allerdings auch elektronische Fernsignaturen vor, sodass Signaturen beim Vertrauensdiensteanbieter erzeugt und

gespeichert werden können (siehe Erwägungsgrund 52, eIDAS-Verordnung).
Die Folgen dieser Regelungen sind aus datenschutzrechtlicher Sicht derzeit noch nicht abzuschätzen. Das hohe Datenschutzniveau in Deutschland hatte bisher sichergestellt, dass für die Signaturerstellung von qualifizierten elektronischen Signaturen bisher nur bei der Bundesnetzagentur gelistete Produkte verwendet werden durften. Mit der nun eingeführten Fernsignatur ist es dem Antragsteller nicht möglich, zu prüfen, ob seine Signatur auch gemäß dem neuesten Stand der Technik erstellt wurde. Es besteht durchaus die Gefahr, dass der Nutzer nun unwissentlich schlechtere Verfahren auswählt, weil sie preisgünstiger sind.
Interessant für den Nutzer von qualifizierten elektronischen Signaturen könnte auch das „Aussetzen qualifizierter Zertifikate“, also das Sperren des oben genannten elektronischen Zertifikates sein. So ist es nun laut eIDAS möglich, bspw. für einen genauen Zeitraum ein qualifiziertes Zertifikat für die qualifizierte elektronische Signatur sperren zu lassen. Aus der qualifizierten elektronischen Signatur wird damit nur noch eine normale elektronische Signatur. Wie oben beschrieben, ist dann eine rechtsverbindliche elektronische Unterschrift nicht möglich, da zu der elektronischen Signatur die dazugehörige Personenüberprüfung mangels gesperrten Zertifikats nicht vorgenommen werden kann.
Denkbar ist ein solches Szenario bspw. dann, wenn man den Datenträger mit seiner qualifizierten elektronischen Signatur verlegt hat und sicherstellen möchte, dass bis zum Wiederauffinden mit diesem Datenträger kein Missbrauch geschieht, also elektronische Dokumente nicht im eigenen Namen einfach von Dritten unterschrieben werden.
Die EU-Verordnung eIDAS regelt aber nicht nur die Anforderungen an qualifizierte Zertifikate für elektronische Signaturen, elektronische Siegel und für die Authentifizierung der Website, sondern auch Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten.

Durch die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014), wurde für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben. Diese gilt es umzusetzen.

14.7 Betriebssysteme mit Cloud Anbindung – immer online

„Daten in der Cloud“ sind in aller Munde, und unsere Gesellschaft hat diesen Begriff in den täglichen Gebrauch aufgenommen. Doch was ist eine Cloud? Und was hat sie mit Betriebssystemen zu tun?
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete bereits im 10. Tätigkeitsbericht (Beitrag 14.4) über die Risiken des Cloud Computing. Allgemein gesprochen ist die „Cloud“ ein Ersatzkonstrukt, welches Datenspeicherung und -verarbeitung von lokalen Geräten wie PCs, Laptops, Tablets und auch Smartphones in den Bereich des Internets auslagert. Der Nutzer erfährt gar nicht mehr, wo genau seine Daten gespeichert sind. Und genau dieses unscharfe Wissen, wo was verarbeitet wird, prägt den Begriff der Cloud (oder auch der Wolke). Die Vorteile liegen für den Nutzer dabei auf der Hand: Er muss sich nicht um Details kümmern. So ist es normal geworden, von überall Zugang zu Mails, Kurznachrichten, Kartendiensten oder Sprachassistenten zu haben. Auch Fotos und Musikbibliotheken werden zunehmend nicht mehr auf dem Gerät, sondern in der Cloud gespeichert, damit sie von überall und auch mittels verschiedener Geräte abrufbar sind. Aber auch Unternehmen und öffentliche Stellen nutzen vermehrt Cloud-Dienste bewusst oder unbewusst.
Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste und der Wirtschaftsspionage, empfahl der TLfDI bei der Nutzung von Cloud-Diensten generell deutsche oder europäische Cloud-Anbieter vorzuziehen, die zudem von vertrauenswürdigen Stellen zertifiziert sind (10. Tätigkeitbericht Beitrag Nummer 14.4).
Nachfolgend wird hier nun insbesondere die neue Entwicklung der Integration von Cloud-Funktionen in Betriebssystemen behandelt und unter Beitrag Nummer 14.11 dieses Tätigkeitsberichtes auch auf die Änderungen der Orientierungshilfe Cloud Computing V2.0 eingegangen.
Aus der Sammlung und Aufbereitung von Datenspuren zur Bildung von Personenprofilen ist in den letzten Jahren ein großer Markt entstanden, und von diesem Markt wollen die großen Hersteller von Betriebssystemen nun auch profitieren. Bisher stellten Betriebssysteme Grundfunktionen wie Speichern und Laden von Daten, Ausführen von Programmen auf dem Gerät und die Kommunikationsmög-

lichkeit mit anderen Geräten zur Verfügung. Einige Betriebssystemhersteller bieten nun zum Teil auch schon Online-Funktionen wie die Internetsuche über Sprachbefehle, zentrale Terminplaner, Kartendienste oder das Speichern von Daten auf einem Speicherplatz „in der Cloud“ an. Dadurch kann das Verhalten der Benutzer von ihnen besser nachvollzogen und im Detail analysiert werden. Leider unterliegen die Betriebssystemanbieter dabei oft nicht dem deutschen oder europäischen Datenschutzrecht.

Aus datenschutzrechtlicher Sicht bergen cloudunterstützte Betriebssysteme generell Datenschutzrisiken. Einer der Kritikpunkte sind dabei die Standardeinstellungen. Diese sind meist so gewählt, dass der Betriebssystemhersteller schon bei der ersten Inbetriebnahme sehr viele Daten erfasst. Das Datenschutzprinzip, dass die Standardeinstellungen bei der Inbetriebnahme des Systems vom Hersteller so gewählt werden, dass möglichst wenig Daten übermittelt werden (Privacy-by-Default), wird hier weitestgehend ignoriert.

Das Fenster zur Privatsphäre ist somit geöffnet.

So konnte man im August 2015 der Fachpresse entnehmen, dass nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail-Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten sofort an Microsoft übertragen werden. Außerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich“ angesehen wird (siehe dazu http://www.microsoft.com/de-de/privacystatement/default.aspx). Aus diesem Grund hatte der TLfDI noch im gleichen Monat eine entsprechende Pressemitteilung veröffentlicht:

(https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pressemitteilung_windows_10.pdf, siehe Anlage 22). In dieser wurde auf die Notwendigkeit hingewiesen, selbst noch persönliche Einstellungen vorzunehmen, um die eigene Privatsphäre zu schützen. Dabei wurde gleich ein entsprechender externer Link zu Tipps zur Verbesserung der Einstellungen bei Windows 10 veröffentlicht. Dadurch

konnten Bürger zeitnah durch Selbsthilfe ihr Betriebssystem datenschutzgerechter einstellen.
Auch die 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahm sich dann im Oktober 2015 des Themas der cloudunterstützten Betriebssysteme an und zeigte in der Entschließung „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ die entsprechenden Datenschutzrisiken auf (siehe Anlage 16).
So können nach Angaben der Konferenz weitreichende Datenverarbeitungsbefugnisse nicht dadurch gerechtfertigt werden, dass Nutzer auf Basis der Zustimmung zu AGB datenschutzunfreundlichen Voreinstellungen implizit zustimmen würden. Auch das Ermöglichen einer Opt-Out-Lösung wird nicht als zielführend angesehen, d. h., das manuelle Abschalten der Dienste im Nachhinein ist keine datenschutzfreundliche Lösung. Systeme dürfen nicht einfach Daten erfassen und im Nachhinein fragen, ob man es nicht will, sondern müssen vorab fragen, ob man dieser Datenerfassung zustimmt (Opt-In-Lösung). Hier bedarf es technisch unterstützter Einwilligungslösungen, die vor der Inbetriebnahme greifen müssen. Für jeden Dienst muss theoretisch eine Einwilligung (und auch die Möglichkeit des Widerrufs) gegeben werden. Der Widerruf ist momentan nur durch das Finden und Nutzen der entsprechenden Einstellungen möglich und damit ein sehr mühsamer Weg. Die Konferenz fordert daher die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Weiterhin empfiehlt die Datenschutzkonferenz in der oben genannten Entschließung den Benutzern der neuen Betriebssysteme, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen.

Moderne Betriebssysteme bieten heutzutage viele Cloud-Funktionalitäten an. Dabei sind die Standardeinstellungen selten datenschutzgerecht; Privacy-by-default wird daher nicht umgesetzt. Der Nutzer muss sich momentan selber behelfen und durch Recherche die möglichen Einstellvarianten finden. Der rechtliche Mechanismus der Einwilligung und des Widerrufs ist technisch noch unzureichend umgesetzt und zu kompliziert. Damit sind viele Betriebssysteme heute Datenschleudern-by-default.

14.8 Problem: Biometrische Gesichtserkennung

Biometrische Gesichtserkennungen sind auf dem Vormarsch. Für diesen Zweck müssen vom Gesicht des Nutzers Merkmale berechnet werden, welche beim ersten Erkennungsvorgang dann einer Person zugeordnet werden. Diese erfassten biometrischen Merkmale bilden danach die Grundlage für eine spätere Wiedererkennung. Der Trend geht bspw. dahin, dass man sich mit dieser Technik dann an Geräten anmelden kann, indem bei der jeweiligen Anmeldung das Gesicht erneut erfasst und mit den bereits gespeicherten biometrischen Merkmalen verglichen wird. Ist der Vergleich positiv, erfolgt die Anmeldung nutzerbezogen am Gerät.
Pech für den, der gerade eine Gesichts-OP hatte, oder wenn eine andere Person unberechtigt vom Berechtigten, bspw. im Schlaf oder im Vollrausch, vor dem jeweiligen Gerät diese Funktion auslöst, um den unberechtigten Zugang bspw. zum Handy und den darauf gespeicherten Mails zu bekommen.
Aber Spaß beiseite!

Die Gesichtserkennung ist unter anderem auch geeignet, Begehrlichkeiten beim Arbeitgeber zu wecken, den Zugang zu sensiblen Bereichen per Gesichtserkennung zu regeln und kontrollieren zu können. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte schon am 23. Mai 2013 in der Pressemitteilung „Nur mit dem Fingerabdruck zum Arbeitsplatz?“ darauf hingewiesen, dass die Erhebung, Speicherung und Verwendung biometrischer Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der ArbeitnehmerInnen darstellt, der datenschutzrechtlich nicht gerechtfertigt ist. Nur in besonderen Einzelfällen kann eine biometrische Zutritts- oder Zugriffskontrolle am Arbeitsplatz unter strengen Voraussetzungen zulässig sein.
Aus datenschutzrechtlicher Sicht haben alle oben genannten Beispiele gemeinsam, dass sich Nutzer überlegen sollten, ob sie diese Funktionalität wirklich selbst wollen oder lieber darauf verzichten sollten. In ihren Überlegungen sollten sie auch prüfen, ob die biometrischen Merkmale verschlüsselt abgespeichert und vor unberechtigtem Zugriff Dritter geschützt sind.
Biometrische Gesichtserkennungen werden aber auch in sozialen Netzwerken zunehmen. Schon jetzt ist es üblich, dass man bspw. bei (Gruppen-)Fotos eine Person markieren und dieser Markierung einen

bestimmten Namen zuweisen kann. Es gibt auch bereits Software, die aufgrund einer Markierung auf einem Foto dann den ganzen Datenbestand durchsuchen kann, auf welchen Fotos diese Person noch zu sehen ist. Im privaten Hausgebrauch scheint dies auch eine nützliche Software. Diese Funktionalität – von Betreibern sozialer Netzwerke in ihren sozialen Netzwerken eingesetzt – bietet allerdings dann die Möglichkeit einer Komplettdurchsuchung aller gespeicherten Fotos in der Datenbank des sozialen Netzwerkes. Sowohl für die Profilbildung, die Betreiber sozialer Netzwerke gerne für ihre eigenen Interessen optimieren wollen, als auch für jegliche Sicherheitsbehörden können solche Gesichtserkennungsprogramme hochinteressant werden.

Aus diesem Grund hatte die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2014 in einer Entschließung „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“ auch noch einmal auf die erforderliche Einwilligungserklärung des Betroffenen hingewiesen (siehe Anlage 13).
Eine der wichtigsten Forderungen ist, dass über jegliche biometrische Gesichtserkennung der Betroffene in der Regel vorher informiert wird und sie nur mit Einwilligung des Betroffenen erfolgen darf.

Eine biometrische Gesichtserkennung zur Zugangskontrolle zu Geräten und zu Räumen scheint auf den ersten Blick eine optimale Lösung, bedarf aber einer vorhergehenden Einwilligung des Betroffenen. Auch soziale Netzwerke haben die Vorteile der Gesichtserkennung für ihre Zwecke erkannt. Aber auch hier bedarf es in jedem Fall der vorhergehenden Einwilligung des Betroffenen. Weiterhin sind die gespeicherten biometrischen Merkmale verschlüsselt zu speichern und der Zugriff von Dritten auszuschließen.

14.9 Newsletter – immer datenschutzgerecht?

Um Informationen an eine bestimmte Zielgruppe regelmäßig oder schnell verteilen zu können, bedient man sich gerne so genannter Newsletter. Newsletter werden in der Regel einmalig versendet. Dennoch ist es nicht unüblich, die versendeten Newsletter für einen späteren Abruf noch einmal auf der entsprechenden Website bereit-

zustellen. Newsletter mit personenbezogenen Daten unterliegen dabei datenschutzrechtlichen Vorschriften. Werden sie nachträglich gespeichert, sind weitere datenschutzrechtliche Vorgaben zu beachten.

Im vorliegenden Fall hatte eine verantwortliche Stelle auf ihrer Webseite die Newsletter gespeichert, um sie für eventuelle Abrufe bereitzuhalten. In einem dieser Newsletter waren allerdings auch Fotos von Mitarbeitern und deren Namen veröffentlicht.

Ein ehemaliger Mitarbeiter forderte nun, sein Foto und den Namen aus dem Newsletter von der Webseite zu löschen. Alle Versuche, dies beim ehemaligen Arbeitnehmer durchzusetzen, schlugen jedoch fehl, sodass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hinzugezogen wurde.

Nachdem der TLfDI die Sachlage prüfte und die verantwortliche Stelle kontaktierte, teilte diese mit, alle Fotos des Beschwerdeführers „bei sich“ gelöscht zu haben. Der TLfDI stellte jedoch fest, dass der betroffene Newsletter nach wie vor in der Original-Version abrufbar war. Es stellte sich heraus, dass lediglich alle Links zum Newsletter auf der Webseite gelöscht worden waren. So musste der TLfDI erneut nachhaken und auf Umsetzung drängen. Dem Mangel wurde nun abgeholfen, indem der gesamte Newsletter gelöscht wurde.

Grundsätzlich sind Internetlinks nur Verweise auf Dokumente (wie Webseiten oder eben auch Newsletter), die den Ort und den Namen des Dokumentes im Internet anzeigen. Mit der Löschung des Hinweises auf ein Dokument verschwindet nicht das Dokument selber. Dieses ist unverändert vorhanden. Bei Löschungsbedarf muss also das Original-Dokument gelöscht werden und nicht (nur) alle Verweise darauf.

Die Löschung erfolgte nicht nur aufgrund von „good will“, sondern es bestand tatsächlich eine Verpflichtung hierzu. Eine konkrete Rechtsgrundlage für die Veröffentlichung von Mitarbeiterfotos war in diesem Zusammenhang nicht ersichtlich. Daher kann die namentliche Veröffentlichung von Mitarbeitern nur mit deren Einwilligung erfolgen (§ 4 Thüringer Datenschutzgesetz).

In der Vergangenheit wurden die Mitarbeiter bei der Aufnahme der Beschäftigung lediglich darauf hingewiesen, dass für den Newsletter und im Rahmen von Veranstaltungen Fotos aufgenommen und ggf. veröffentlicht werden. Soll eine Veröffentlichung im Internet erfolgen, ist das Foto weltweit abrufbar. Eine unberechtigte Weiterverwendung oder Veränderung durch Dritte kann daher nicht generell

ausgeschlossen werden. Als Mitarbeiter sollte man daher vorher immer reiflich abwägen, ob man mit der Veröffentlichung von Fotos im Internet einverstanden ist.

Eine Löschung von Links auf abrufbare Dokumente im Internet, verursacht noch keine Löschung von Daten in einem Dokument selbst. Nur eine Löschung im Original-Dokument ist hier zielführend. Einwilligungserklärungen müssen zweckgebunden oder besser noch fallbezogen eingeholt werden, sonst sind sie rechtlich unwirksam.

14.10 Verschlüsselung mit TrueCrypt

Lange galt TrueCrypt als sicheres Programm zum Verschlüsseln von Daten auf der Festplatte, auf Datenträgern oder aber auch zum Verschlüsseln der Daten vor einer Datenübermittlung. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl dieses Programm. Doch die Weiterentwicklung dieses Programms wurde durch die Entwickler Ende Mai 2014 eingestellt, sodass nunmehr keine Empfehlung seitens des BSI mehr erfolgt.
Da einige Programmteile von TrueCrypt auch in anderen Programmen verwendet werden, hatte das BSI das Fraunhofer-Institut für sichere Informationstechnologie (SIT) mit der Durchführung einer Sicherheitsanalyse von TrueCrypt in der Version 7.1a beauftragt. Das Ergebnis dieser Sicherheitsanalyse wurde vom BSI im November 2015 unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2 veröffentlicht.

In der Studie wird u.a. festgestellt, dass TrueCrypt nur dann noch einen wirksamen Schutz entfaltet, wenn das Gerät, auf dem die Daten gespeichert sind, sich im ausgeschalteten Modus befinden. Dies ist bspw. bei Verlust des USB-Sticks oder Laptops der Fall.
Die Studie kommt zum Schluss, dass in den anderen Fällen, also bspw. im Online-Modus, kein sicherer Schutz mehr besteht. Grund dafür ist, dass der Einsatz eines heimlich installierten Key-Logger-Programms, also eines Programmes, welches die Eingabe an der Tastatur mitschneidet, den Schutz unterlaufen könnte. Ebenso kann

andere installierte Schadsoftware den Schutz von TrueCrypt unterlaufen.
Was bedeutet dies nun für die Anwender? Wieso wird hier auf einmal die Gefahr des Key-Loggers problematisiert und bei anderen sicherheitsrelevanten Prozessen bewusst ausgeblendet?
Die Datenschutzbeauftragten des Bundes und der Länder haben beispielsweise bei der Einführung des elektronisch lesbaren Personalausweises die unsicheren Lesegeräte ohne eigenständige Tastatur genau aus diesem Grund kritisiert und vor Key-Loggern gewarnt. Weder die Bundesregierung noch das BSI änderten daraufhin das Verfahren dahingehend, dass nur Lesegeräte mit eigener Tastatur zugelassen werden.
Auch darf der Bürger sich fragen, wenn er die von der Bundesregierung favorisierte De-Mail benutzt, ob diese vor einem Key-Logger geschützt ist. Diesbezügliche Aussagen sind für den Bürger derzeit nicht zu finden.
Welche Alternative schlägt nun das BSI hinsichtlich TrueCrypt vor? Muss man gänzlich auf TrueCrypt verzichten? Aus datenschutzrechtlicher Sicht ergibt sich aus der vorliegenden Sicherheitsanalyse, dass TrueCrypt durchaus weiter Anwendung finden kann, wenn die Daten auf einem Gerät nur bei Verlust oder Diebstahl des Gerätes vor unberechtigtem Zugriff gesichert werden sollen. Auch für ausgelagerte Datensicherungen scheint es gemäß der oben zitierten Studie des Fraunhofer-Instituts weiterhin geeignet. Nur für den Zugriff auf Daten in laufenden Systemen kann die Verschlüsselung allein keinen ausreichenden Schutz gewährleisten.
Man muss also vor dem Einsatz immer schauen, welche Empfehlungen derzeit das BSI ausspricht (www.bsi.de). Wichtig ist, dass man immer dem Stand der Technik entsprechende Verschlüsselungssoftware einsetzt, um nicht fahrlässig zu handeln.

Verschlüsselungssoftware ist immer entsprechend dem aktuellen Stand der Technik einzusetzen. Daher sollte man sich regelmäßig beim Bundesamt für Sicherheit in der Informationstechnik (BSI) informieren.

14.11 Cloud-Computing 2.0 und Safe Harbor

Zur datenschutzkonformen Gestaltung und zur Nutzung von Cloud Computing hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits 2011 eine Entschließung veröffentlicht. Damals wurde parallel zur Entschließung auch eine entsprechende Orientierungshilfe (OH) erarbeitet (siehe 9. TB, Pkt. 14.1). Diese Orientierungshilfe richtet sich sowohl an die Anbieter von Cloud-Diensten als auch an deren Nutzer.

Aufgrund der technischen Entwicklung und aufgrund der NSA-Affäre wurde sie drei Jahre später überarbeitet und 2014 unter „Cloud-Computing 2.0“ veröffentlicht:
https://www.tlfdi.de/imperia/md/content/datenschutz/themen/orientierungshilfen/oh_cc_2.0.pdf.

Die OH „Cloud-Computing 2.0“ geht nun neben dem grenzüberschreitenden Datenverkehr auch auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA) ein. Es wird darauf hingewiesen, dass es für die Zugriffsbefugnisse der US-Behörden nicht maßgebend ist, ob sich die Cloud innerhalb oder außerhalb der USA befindet. Es wird nach US-Recht als ausreichend angesehen, wenn der Cloud-Anbieter zumindest auch in den USA geschäftlich tätig ist.

Aus datenschutzrechtlicher Sicht steht eine entsprechende Datenübermittlung von Unternehmen mit Sitz in Europa bzw. Deutschland an US-Behörden nicht mit Art. 26 der Richtlinie 95/46/EG bzw. § 4c BDSG im Einklang. Zudem würde bei einer entsprechenden Datenübermittlung durch den Cloud-Anbieter auch der Cloud-Anwender automatisch gegen europäisches und deutsches Datenschutzrecht verstoßen, da er in seiner datenschutzrechtlichen Verantwortlichkeit bleibt. Letzteres ergibt sich aus der Tatsache, dass bei Auftragsdatenverarbeitung der Auftraggeber verantwortliche Stelle bleibt. Die OH weist deshalb darauf hin, dass derzeit ein internationales Übereinkommen fehle, welches eine solche Datenübermittlung an US-Behörden rechtfertige.

Auch in den USA ansässige Cloud-Anbieter, die sich dem Safe-Harbor-Abkommen zwischen der EU und den USA angeschlossen

hatten, waren von diesem staatlichen Eingriff durch US-Behörden nicht ausgenommen.
Das Safe-Harbor-Abkommen ist bekanntlich am 6. Oktober 2015 vom Europäischen Gerichtshof (EuGH, C-362/14) für ungültig erklärt worden, da die USA ein angemessenes Schutzniveau übermittelter personenbezogener Daten nicht gewährleisten. Dies wurde u. a. damit begründet, dass der Zugriff von Behörden, der generell auf den Inhalt elektronischer Kommunikation zielt, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt (siehe dazu Nummer 2.1.).
So ist die derzeitige Orientierungshilfe Cloud-Computing in ihrer Version 2.0 nun unter Beachtung dieses Urteils anzuwenden und die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA zu unterlassen.

Diese Orientierungshilfe Cloud-Computing 2.0 ist nicht nur in ihrer geänderten Fassung von 2014 anzuwenden, sondern auch unter Beachtung der Entscheidung des Europäischen Gerichtshofes (EuGH) zu Safe Harbor. Die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA ist daher bis auf weiteres zu unterlassen.

14.12 Telemediengesetz (TMG) – zeitgemäß?

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Die Datenschutzbeauftragten des Bundes und der Länder monierten allerdings in ihrer Umlaufentschließung vom 5. Februar 2015, dass das Telemediengesetz bezüglich des Setzens von Cookies nicht der Europäischen Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) entspricht. Denn die E-Privacy-Richtlinie gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, nur, wenn der Nutzer dazu seine Einwilligung gegeben hat und auch hinsichtlich der Notwendigkeit der Speicherung eine Information erfolgte. Dieses ist, nach Meinung der Datenschutzbeauftragten, im Telemediengesetz (TMG) nicht umgesetzt, da § 15 Abs. 3 TMG regelt, dass der Nutzer nur auf sein Widerspruchsrecht hinzuweisen ist.
Ein weiteres Problem ist, dass mit der fortschreitenden Digitalisierung auch das Bedürfnis nach öffentlichem Zugang im Internet unter

Nutzung frei zugänglicher drahtloser Netzwerke (WLANs) besteht. So wurde auch beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage nach der Haftung (Störerhaftung) gestellt und welche Risiken sich damit verbinden. Das Problem dabei ist, dass die „Störerhaftung“ dann eintritt, wenn über ein zur Verfügung gestelltes WLAN eine Rechtsverletzung begangen wurde.
Hintergrund für die unsichere Rechtslage sind § 8 TMG und verschiedene Urteile des BGHs zur Störerhaftung. Um im Nachhinein die Störerhaftung weitestgehend zu minimieren bzw. gänzlich auszuschließen, bieten viele Anbieter den Internetzugang über WLAN nur mit einem zugewiesenen Account an – oft verbunden mit der Eingabe weiterer Daten. Dies wird z. B. in Hotels, Flughäfen, Zügen, Straßenbahnen, Fernbussen oder auch in Cafés genutzt.
Aufgrund der Störerhaftung sind deshalb „offene“ WLANs, die ohne Anmeldung einen Zugriff auf das Internet ermöglichen, in Deutschland sehr selten anzutreffen.
Auslöser einer Störhaftung kann bspw. eine Verletzung des Urheberrechts sein, wie beim Filesharing im Video - und Musikbereich.
Gemäß § 8 Telemediengesetz sind von der Haftung als Störer derzeit nur Internet-Provider ausgenommen. Rechtlich ungeregelt ist daher derzeit die Anwendbarkeit des § 8 TMG hinsichtlich der Haftung privater, geschäftsmäßiger und öffentlicher Anbieter.
Dies hat auch die Bundesregierung erkannt und, um die nötige Rechtssicherheit in Haftungsfragen zu verschaffen, am 18. November 2015 einen „Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes“ vorgelegt (BT DS 18/6745).
Der TLfDI empfiehlt daher, das Gesetzgebungsverfahren abzuwarten und wird die Probleme weiter im Blick haben.

Das Telekommunikationsgesetz bedarf hinsichtlich der europäischen Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) einer Klarstellung.
Auch sollte das Betreiben frei zugänglicher drahtloser Netzwerke (WLANs) rechtsicher geregelt werden. Dabei sollte auch die Sicherheit der Netzwerkanbindung dem aktuellen Stand der Technik entsprechen.

14.13 Windows XP – baufällig ...

Seit dem 8. April 2014 werden vom Hersteller Microsoft Corporation (Microsoft) für das Betriebssystem Windows XP auch keine Sicherheits-Updates mehr für den erweiterten Support geliefert. Microsoft hatte diesen Fakt bereits Ende 2002 angekündigt und grundlegende Supports schon 2009 eingestellt. Immerhin war das Betriebssystem dreizehn Jahre alt.
Dies birgt für Benutzer, die das Betriebssystem weiterhin benutzen, erhebliche Risiken. Zu vergleichen ist das mit einem alten, maroden Haus, in dem nun die immer wieder eingeworfenen Fensterscheiben nicht mehr mit neuem Sicherheitsglas ausgerüstet werden. Nur so kann ein Glaser (gemeint: der Software-Hersteller Microsoft) dem Zahn der Zeit (gemeint: dem Stand der technischen Entwicklung) trotzen und dem Verfall Einhalt gebieten.
Wo liegen die Probleme?
Aufgrund der fehlenden Sicherheits-Updates durch Microsoft sind personenbezogene Daten auf Windows XP-Rechnern einem unverantwortlich hohen Risiko möglicher Hacker-Angriffe ausgesetzt.
Nachdem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr, dass trotz der Abkündigung von Windows XP ein Jahr später immer noch Windows XP-Rechner im Einsatz sein könnten, wandte sich der TLfDI an das Thüringer Innenministerium als kommunale Aufsichtsbehörde mit der Bitte, die Kommunen auf die Risiken beim Einsatz von Windows XP hinzuweisen. Dieses wurde auf wiederholtes Bitten viele Monate später umgesetzt.
Zum anderen wies der TLfDI die obersten Landesbehörden auf die entsprechenden Gefahren hin. Er bat um Rückinformationen, wie viele PCs in den Ressorts noch mit dem alten Betriebssystem arbeiteten. Wenn mit solchen Rechnern noch personenbezogene Daten verarbeitet würden, sollten diese in der Thüringer Landesverwaltung dringend umgestellt bzw. abgeschaltet werden.
Im Ergebnis teilten die Ministerien für sich und ihre jeweils nachgeordneten Bereiche mit, dass die Windows XP-Rechner zum Großteil zeitnah abgelöst werden sollen. Allerdings werden – selbst bei Einhaltung der Zeitpläne der Ministerien – nach Redaktionsschluss des vorliegenden Tätigkeitsberichtes ca. 300 Windows XP-Rechner in der Thüringer Landesverwaltung im Einsatz sein. Davon werden die meisten in Entwicklungs- bzw. Servicebereichen, in der Lehre oder aber als Messplatz-PCs unter sehr speziellen Einsatzbedingungen verwendet. Hauptgrund dafür ist, dass einige Systeme wegen Soft-

ware-Unverträglichkeiten (fachenglisch: Inkompatibilität) – insbesondere bei verwendeten älteren Fachverfahren oder aber in medizinischen Geräteumgebungen – nicht mit den neueren Betriebssystemen zusammenarbeiten. Hier müssen Kompromisse geschlossen und Übergangslösungen gefunden werden.
Sollen XP-Rechner weiterhin im Einsatz verbleiben, so ist es notwendig, sie in „abgeschotteten Systemen“ zu betreiben. Das sind solche Systeme, in denen das Betriebssystem über Browserfunktionen beispielsweise keine aktive Verbindung zum Internet herstellt. Um die Funktionsfähigkeit als abgeschottete Systeme zu gewährleisten, sind explizit technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen zu treffen. Nur so können Sicherheitsrisiken minimiert werden. Eine dieser TOM ist, Einstellungen im Browser oder am Proxy so vorzunehmen, dass der PC keine Internetverbindung aufbauen kann. Aber auch organisatorische Regelungen, wie beispielsweise Dienstanweisungen, zählen zu den TOM. Darin sollte eindeutig vorgeschrieben werden, dass keine Windows XP-Rechner mehr einen Internetzugang besitzen dürfen und zeitnah ausgetauscht werden sollten. Bei Windows XP-Rechnern, die wegen spezieller Fachverfahren derzeit immer noch nicht einfach umgestellt werden können, bedarf es zusätzlich einer konkreten Planung mit dem Hersteller dieser Fachverfahren-Software, um die Umstellung der alten auf neuere Software zeitnah zu realisieren.
Mittelfristig bleibt im übertragenen Sinne zum Abriss des alten, maroden Hauses jedoch keine zukunftsorientierte Alternative. Das Betriebssystem Windows XP ist deshalb zeitnah und flächendeckend durch neuere Betriebssysteme zu ersetzen.
Dies wurde auch von den obersten Landesbehörden erkannt und eine Umstellung mittelfristig zugesichert.

Das Client-Betriebssystem Windows XP erhält seit April 2014 im erweiterten Support keine Sicherheits-Updates mehr. Es ist daher durch neuere Client-Betriebssysteme zu ersetzen.
Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.

Datenschutz – © Gesina Ottner / Fotolia.com

15 Veranstaltungen

15.1 Maus-Liebhaber: Gesucht und gefunden!

Knapp 50 Seniorinnen und Senioren waren im September 2015 dem Vorschlag des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gefolgt, sich zur Gründung einer Interessengruppe „SeniorenComputerClub“ (SCC) beim Schutzbund der Senioren und Vorruheständler Thüringen e. V. in Erfurt einzufinden. Dieses positive Echo zeigte, dass sich auch Menschen im fortgeschrittenen Alter intensiv mit der digitalen Technik befassen und gern gemeinsam über Neuigkeiten und Probleme diskutieren und zu neuen Erkenntnissen kommen wollen. In Anwesenheit von Dr. Lutz Hasse, stellten Detlef Wagner (Informatiklehrer) und Marianne Schwalbe (Leiterin des Senioren-Schutzbundes) das Konzept des Clubs vor. Innerhalb des Clubs wurden vier Interessengruppen gebildet, die sich mit den Themen Bild/Film/Musik, Internet, soziale Netzwerke und Windows 10 beschäftigen werden. Eine weitere Gruppe fand sich unter der Bezeichnung „Zum Neustart entschlossen“ zusammen, die sich – wieder – mit dem Thema Computer auseinandersetzen wollte. Dr. Lutz Hasse stellte in seinem Beitrag die Bedeutung des Internets als Faktor der Lebensqualität mit all seinen Fallen und den erforderlichen Vorsichtsmaßnahmen heraus. Ziel ist es, sich zu rechtlichen (z. B. Urheberrecht, Bildrechte usw.), technischen und anderen relevanten Aspekten auszutauschen. Näheres finden Sie unter http://www.seniorenschutzbund.org/cms/front_content.php.

Das Anliegen ist es, gemeinsam zu tüfteln und zu üben, Kenntnisse zu vertiefen und Erfahrungen auszutauschen. Der TLfDI will mit dieser Kooperation den Erwerb von Medienkompetenz für Seniorinnen und Senioren ermöglichen und Silver Surfer im Netz für den notwendigen Schutz ihrer Daten im Internet sensibilisieren.

15.2 Der TLfDI kommuniziert!

Ein Internet-Forum für Krankenhäuser, die Vorratsdatenspeicherung, Digitale Selbstverteidigung, „Unsafe“ Harbor, Krankenkassen als Fitnesscoach oder Algorithmen Allmächtig – die Presse- und Öffentlichkeitsarbeit ist für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein wichtiges Instrumentarium, um die datenschutzrechtlichen Themen auch außerhalb der Behörde zu kommunizieren. Die Öffentlichkeitsarbeit organisiert den Kontakt zwischen dem TLfDI und dem Bürger. Durch sie erreicht der TLfDI die Aufmerksamkeit breiter Bevölkerungsschichten, um diese für datenschutzrechtliche Themen zu sensibilisieren. Seit Mai 2015 gibt es beim TLfDI einen eigenständigen Arbeitsbereich für Öffentlichkeitsarbeit und Presse, da dieses Gebiet nicht mehr nur nebenbei erledigt werden konnte. Dieser Bereich ist zuständig für die Medien, er koordiniert die eingehenden Presseanfragen und ist für die Pressekonferenzen sowie die Vorbereitungen von Veranstaltungen des TLfDI zuständig. Er unterstützt den TLfDI bei allen öffentlichen Auftritten und den aktuellen Pressemitteilungen und betreut den Internetauftritt. Im Berichtszeitraum wurden 48 (!) Pressemitteilungen beim Datenschutz, siehe ab Anlage 18, veröffentlicht. Vier Pressekonferenzen wurden abgehalten. In knapp zweihundert Beiträgen wurde in den aktuellen Medien im Berichtszeitraum über die Tätigkeit des TLfDI berichtet. In der Anlage 38 finden Sie drei der markantesten Ereignisse, nachzulesen auch auf der Internetseite www.tlfdi.de. Im kommenden Berichtszeitraum wird sich die Website einem Relaunch unterziehen, um bedienfreundlicher und zeitgemäßer zu werden.

Seit Mai 2015 gibt es beim TLfDI einen eigenständigen Arbeitsbereich für Öffentlichkeitsarbeit und Presse. Die für den nicht-öffentlichen Bereich relevanten Pressemitteilungen des TLfDI finden Sie im Anhang.

Update – © Marco2811 / Fotolia.com

16 Vorträge – Der TLfDI ist unterwegs!

Ob Datenschutz in Unternehmen oder in medizinischen Einrichtungen, ob Videoüberwachung, Vorratsdatenspeicherung oder die Frage nach dem Umgang mit sozialen Netzwerken – datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Indikatoren sind nicht nur die vielfältigen Eingaben von Bürgerinnen und Bürgern, sondern vor allem auch das gesteigerte Interesse der Medien an datenschutzrechtlichen Themen aller Art. Es vergeht kaum ein Tag, an dem der Schutz der persönlichen Daten nicht in den Nachrichten oder Medien auftaucht. Fast täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herein, ob der TLfDI nicht mit einem "Rundum-sorglos-Paket" für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung durch seine Vorträge unterstützen kann. Der TLfDI selbst und einige seiner Mitarbeiter haben im Berichtszeitraum an mehr als 50 (!) Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im nicht-öffentlichen Bereich finden Sie ab Anlage 24.

Nicht verzagen, TLfDI fragen! Der TLfDI freut sich über das gesteigerte Interesse am Schutz der in der Tat bedrohten Privatsphäre und versucht im Rahmen seiner Möglichkeiten die Bürgerinnen und Bürger, die Mitarbeiter der Schulen und Unternehmen für das Thema Datenschutz in Thüringen zu sensibilisieren und über den neusten Stand seiner Erkenntnisse zu informieren.

Männchen Runder Tisch Business – © fotomek / Fotolia.com

17 Düsseldorfer Kreis

Der Düsseldorfer Kreis ist als Arbeitskreis der Datenschutzkonferenz das oberste Gremium der Aufsichtsbehörden, das sich ausschließlich mit Themen aus dem nicht-öffentlichen Bereich des Datenschutzes befasst. Er fasst Beschlüsse, die die Rechtsauffassung aller Aufsichtsbehörden widerspiegeln oder auf bestimmte datenschutzrechtliche Probleme im Namen aller Aufsichtsbehörden aufmerksam machen sollen. Im Berichtszeitraum hat der Düsseldorfer Kreis folgende Beschlüsse gefasst:

2014

- Beschluss des Düsseldorfer Kreises vom 27. Januar 2014 Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten" (s. Anlage 10)

- Beschluss des Düsseldorfer Kreises vom 19. Februar 2014 Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ (s. Anlage 3)
- Beschluss des Düsseldorfer Kreises vom 26. Februar 2014 Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden (s. Anlage 5)
- Beschluss des Düsseldorfer Kreises vom 26. Februar 2014 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams) (s. Anlage 4)
- Beschluss des Düsseldorfer Kreises vom Mai 2014 Smartes Fernsehen nur mit smartem Datenschutz (s. Anlage 6)
- Beschluss des Düsseldorfer Kreises vom 16. Juni 2014 Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter (s. Anlage 7)

2015

- Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln (s. Anlage 9)
- Videoüberwachung in Schwimmbädern Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises vom 19. Februar 2014, Stand 10. August 2015 (s. Anlage 11)
- Beschluss zur Nutzung von Kameradrohnen durch Private (s. Anlage 8)

Anlagen

Anlage 1

Videoüberwachung –Erfassungsblatt für Kameras

Videoüberwachung - Erfassungsblatt Kameras[1]

Kamera-Bezeichnung (lfd.Nr.) : ……

Hinweis zur Videoüberwachung (ja / nein; wo, wie, verantwortliche Stelle, Rechtsgrundlage):
……
……

Zweck der Kamera: ……
……

Kamera (Typ, Modellbezeichnung) : ……

Auflösung des Kamerabildes (beste angeben):……

Audiofunktion
(vorhanden / ein- / ausgeschaltet) ……

Zoomfunktion (vorhanden/ nicht ~/ verwendet) :
……

Verstell- / Schwenkbereich (vorhanden / nicht ~/ verwendet / Einstellungen):
……
……
.

WLAN-Funktion sowie Internetfähigkeit
(ja: Art der Datenübermittlung > Protokolltyp, Verschlüsselung, Einstellungen // nein) :
……
……

Fernsteuerungsmöglichkeit / Remotezugang zur Kamerasteuerung (ja: Art der Authentifizierung > Protokolltyp, Verschlüsselung, Einstellungen // nein) :
……
……
……

[1] Dieses Erfassungsblatt ist je Kamera auszufüllen und ggfs. zu einer entsprechenden Dokumentation für alle eingesetzten Kameras eines Videoüberwachungssystems zusammen zu fassen.

Änderung des Standard-Zugangs-Passworts: (ja / nein):

……..

Sichtwinkel (ggfs. in Skizze / Lageplan / Zeichnung – S.3 bzw. Anlage – eintragen):

……..

betroffener Personenkreis : ……..

……..

verarbeitungsberechtigte Personen
(wer, wie > z.B. 4-Augen-Prinzip für Einsichtnahme auf angezeigte bzw. gespeicherte Daten; ~ für Kamerasteuerung; Festlegungen, Dokumentation) :

……..

……..

Festlegung der Zugriffsberechtigung / Dokumentation (ja / nein) :

……..

……..

Datum der Inbetriebnahme : ……..

Vorabkontrolle, Sicherheitskonzept :

……..

……..

……..

Einbeziehung des bDSB (sofern vorhanden, ja / nein) :

……..

Maßnahmen:

Beobachtung („verlängertes Auge“, ja / nein) :

……..

Aufzeichnung (ja / nein) : ……..

……..

Speicherfristen (Regelfristen, Begründung für die Dauer) :

……..

……..

Art der Datenlöschung (automatisch, Überschreiben nach … Stunden) :

……..

……..

>Skizze / Lageplan / Zeichnung (S.3 bzw. Anlage)

> Skizze / Lageplan / Zeichnung
(für alle angebrachten Videokameras, Kennzeichnung der beschriebenen Kamera) :

Screenshot der beschriebenen Kamera .
(ggfs. mehrere Ansichten, wenn zoom- bzw. schwenkbar bzw. im seitlichen Winkel veränderlich einstellbar) :

Anlage 2

Checkliste: Liegt ein Fall des § 42a BDSG vor?

Weit hinten im BDSG versteckt, findet man die Regelung des § 42a BDSG, der verantwortliche Stellen unter bestimmten Voraussetzungen dazu verpflichtet, im Falle eines Abhandenkommens von Daten die betroffenen Personen sowie die Aufsichtsbehörde zu informieren. Um verantwortlichen Stellen die Feststellung zu erleichtern, ob ein solcher Fall vorliegt, hat der TLfDI hierfür diese Checkliste erstellt, anhand derer das Vorkommnis eingeordnet werden kann.

❖ Welche Arten von Daten sind erfasst?

Zunächst einmal müssen **personenbezogene Daten** abhanden oder auf andere Weise Dritten zur Kenntnis gekommen sein. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. (§ 3 Abs. 1 BDSG).

Das können etwa äußere Merkmale einer Person sein, wie Größe, Haarfarbe, Gewicht etc. Ebenso erfasst sind geistige Zustände, also z. B. politische Einstellungen, Wünsche oder sexuelle Präferenzen. Auch Verhaltensweisen (etwa Angaben zu Hobbies oder Reisen) und Beziehungen (Vereinsmitgliedschaften, Freunde, Beziehungsstatus) einer Person gehören dazu, ebenso der Name oder die Adresse einer Person.

Allerdings sind nicht alle diese personenbezogenen Daten von § 42a BDSG geschützt, sondern nur folgende besondere Arten:

- **Besondere personenbezogene Daten im Sinne von § 3 Abs. 9 BDSG:**

  Dabei handelt es sich um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Besondere personenbezogene Daten könnten sich zum Beispiel in einer gestohlenen Personalakte eines Arbeitnehmers befinden, in der auch Angaben über dessen Religionszugehörigkeit gemacht wurden.

- **Daten, die einem Berufsgeheimnis unterliegen**

  In bestimmten Berufen dürfen bei der beruflichen Tätigkeit erlangte Informationen nicht weitergegeben werden. Das ist z. B. bei Ärzten, Rechtsanwälten oder Steuerberatern der Fall.

Um solche Daten könnte es sich etwa handeln, wenn ein Anwalt eine Akte versehentlich an einen falschen Mandanten sendet.

- **Personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder entsprechende Verdachtsmomente beziehen**

- **Daten zu Bank- oder Kreditkartenkonten**

Dazu gehören etwa der Name des Kontoinhabers, Kontonummer, Kreditkartennummer, der Name der Bank, oder die PIN-Nummer der Konteninhaber sowie Daten zu deren Umsätzen und Überweisungen.

Das könnte etwa der Fall sein, wenn Kontoauszüge versehentlich an den falschen Empfänger gesendet werden.

❖ **Was muss mit den Daten geschehen sein?**

Es muss ein Vorfall passiert sein, bei dem Daten irgendwie abhanden gekommen sind:

- Dies ist zum einen denkbar durch eine **unrechtmäßige Übermittlung** an Dritte.

Übermitteln an einen Dritten bedeutet, dass die Daten gezielt an jemanden außerhalb der verantwortlichen Stelle bekannt gegeben wurden.

Beispiele dafür sind etwa:

- *Daten werden aus Versehen an Besucher, die versehentlich für Mitarbeiter eines Unternehmens gehalten werden, weitergegeben.*
- *Eine E-Mail oder eine Postsendung, die Daten der o. g. Art enthält, wird falsch adressiert.*
- *Daten werden aus Unkenntnis in ein Land außerhalb der europäischen Union gesendet, das über ein unsicheres Datenschutzniveau verfügt.*

➢ Auch ohne eine gezielte Übermittlung können Daten **unrechtmäßig an Dritte gelangen:**

- *Klassischer Fall ist der Diebstahl von Akten oder Datenträgern, auf denen sich Daten im oben genannten Sinne befinden.*
- *Auch der Zugriff eines Mitarbeiters, der in einem anderen Bereich arbeitet und zum Zugriff auf die bestimmten Daten nicht befugt ist, führt zu dessen unrechtmäßiger Kenntniserlangung.*
- *Ein wichtiger Fall ist auch der versehentliche Verlust von Daten, etwa der Verlust eines Laptops mit den oben genannten Daten im öffentlichen Raum.*

Für die „Kenntniserlangung“ durch einen Dritten muss nicht eindeutig erwiesen sein, dass ein Dritter die Daten tatsächlich gesehen oder ausgewertet hat. Es genügt, wenn eine hohe Wahrscheinlichkeit besteht, dass dies passiert.

❖ **Richtet sich die Norm überhaupt an mich/an mein Unternehmen/meine Organisation?**

Nach § 42a BDSG ist jede „nicht-öffentliche Stelle“ verpflichtet, bei abhandengekommenen Daten Maßnahmen zu ergreifen. Nicht-öffentliche Stellen sind nach § 2 Abs. BDSG „natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts“. Sie können also sowohl als Privatperson als auch als Unternehmen verpflichtet sein. Vo-

raussetzung ist aber weiter, dass Sie bestimmte Arten von Daten bei sich gespeichert haben oder hatten (s. u).
Ebenfalls richtet sich § 42a BDSG an öffentliche Stellen, die nach § 26 Thüringer Datenschutzgesetz den meisten Regelungen des BDSG unterworfen sind.

❖ **Welche Beziehung muss ich/mein Unternehmen/meine Organisation zu diesen Daten haben?**

Sie müssen diese Daten *bei sich* gespeichert haben, d. h., sie auf einem Datenträger erfasst, aufgenommen oder aufbewahrt haben, um sie zu nutzen. Ein Datenträger kann dabei auch Papier sein.
Wenn Sie Daten zwar nicht selbst speichern, dies aber jemand anderes in Ihrem Auftrag tut, gelten Sie nach § 11 BDSG gleichwohl als die speichernde Stelle und sind für die Einhaltung des § 42a BDSG verantwortlich.

❖ **Welche sonstigen Voraussetzungen bestehen, damit ich Benachrichtigungspflichten unterfalle?**

Wenn alle oben beschriebenen Merkmale auf Ihre Situation zutreffen, müssen Sie sich zuletzt fragen, ob durch den Datenverlust schwerwiegende Beeinträchtigungen für die Betroffenen drohen, d. h., ob Personen, auf die sich die Daten beziehen, dadurch irgendwelchen Nachteilen oder Gefahren ausgesetzt sein könnten.
Durch die verantwortliche Stelle ist eine Prognoseentscheidung zu treffen. Sie muss die möglichen Folgen nach Lage der Dinge identifizieren und bewerten. Dabei sollten Sie jedoch keinen allzu hohen Maßstab anlegen. Die Wahrscheinlichkeit, dass Daten veröffentlicht werden oder kriminell genutzt werden, reicht aus. Dies ist bei den betroffenen Datenkategorien fast immer der Fall. Wenn ein solcher Schaden bereits eingetreten ist, müssen Sie keine Abwägung mehr vornehmen.
Wenn Ihre Situation die oben genannten Voraussetzungen erfüllt, müssen Sie sowohl die Aufsichtsbehörde als auch die Betroffenen wie unten beschrieben benachrichtigen.

Wenn Sie im Zweifel sind, ob Benachrichtigungen nach § 42a BDSG erforderlich sind, sollten Sie lieber benachrichtigen bzw. unverzüglich bei der Behörde nachfragen. Denn nach § 47 Abs. 2 Nr. 7 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Eine Zuwiderhandlung kann mit einem Bußgeld geahndet werden.
Wichtig für Sie: Diese Benachrichtigung selbst darf in einem Strafverfahren oder einem Verfahren wegen einer Ordnungswidrigkeit nur gegen Sie als Anzeigeerstatter oder Ihre Angehörigen verwendet werden, wenn Sie es selbst gestatten.

❖ **Wen muss ich wie und wann benachrichtigen, wenn ein Fall des § 42a BDSG vorliegt?**
Die verantwortliche Stelle treffen zweierlei Benachrichtigungspflichten, die sich im Detail voneinander unterscheiden.

➢ **Benachrichtigung der Aufsichtsbehörde**
Zum einen müssen Sie unverzüglich die **Aufsichtsbehörde**, d. h. den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, über diesen Datenverlust informieren. Unverzüglich bedeutet daher, ohne schuldhaftes Zögern. In der Regel geht man hier von einer Frist von drei Tagen aus. In Einzelfällen kann diese aber auch länger sein.
Bitte schildern Sie dabei zunächst, um welche Art von Daten es sich handelt und wie und warum diese abhandengekommen sind.
Zudem sind Sie verpflichtet, der Behörde gegenüber eine **Gefahrenprognose** anzustellen. Dabei müssen Sie angeben, welche nachteiligen Folgen die unrechtmäßige Kenntniserlangung für die Betroffenen haben könnte. Zudem müssen Sie der Behörde gegenüber angeben, was Sie bislang unternommen haben, um diese Folgen zu verhindern oder zumindest abzumildern.

➢ **Benachrichtigung der Betroffenen**
Zum anderen sind Sie verpflichtet, die **Betroffenen** zu informieren, d. h. die Personen, auf die sich die Daten beziehen.
Auch dies muss so schnell wie möglich erfolgen, d. h. unmittelbar nachdem Sie alle „Notfallmaßnahmen“ ergriffen haben, um Schäden zu verhindern.

Auch dabei müssen Sie schildern, was geschehen ist. Zudem sind Sie verpflichtet, den Betroffenen Hilfestellungen zu geben, wie diese sich vor Gefahren schützen können.
Beispiel: Wenn etwa Passwörter verlorengegangen sind, könnten Sie den Betroffenen schildern, wie diese Ihre Konten sperren oder Passwörter ändern können.

Sollten Ihnen die Daten einer so großen Anzahl an Personen abhandengekommen sein, dass die Benachrichtigung jeder einzelnen Person einen unverhältnismäßigen Aufwand darstellen sollte, können Sie alternativ eine öffentliche Benachrichtigung mit den oben genannten Inhalten vornehmen.
Erlaubt ist, die Benachrichtigung in einer Größe von mindestens einer halben Seite in zwei bundesweit erscheinenden Tageszeitungen zu veröffentlichen. Falls Ihnen ein anderes Medium zur Verfügung steht, das die Betroffenen ebenso gut erreicht, etwa eine Website, können Sie auch dieses nutzen.

Wenn Sie unsicher sind: Im Zweifel den TLfDI fragen!

Anlage 3

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

1. Chancen und Risiken einer Videoüberwachung

Videoüberwachung (zum Begriff s. 2.1.1.) ist vermeintlich in der Lage, bei gewissen Sicherheitsproblemen eine einfache Lösung zu bieten. So können etwa unübersichtliche Gebäudekomplexe zu verschiedensten Tages- und Nachtzeiten leicht überwacht werden. Die Aufsicht über das System kann zentral und mit wenig Personalaufwand erfolgen. Die Technik ist erschwinglich und regelmäßig ohne besondere Kenntnisse zu installieren.
Die datenschutzrechtliche Relevanz der Videoüberwachung wird von den Betreibern einer Videoüberwachungsanlage jedoch häufig falsch eingeschätzt. Jeder Mensch hat grundsätzlich das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mithilfe von Kameras beobachtet oder aufgezeichnet wird. Die Tatsache, beobachtet zu werden, kann bei vielen Personen eine Änderung ihres Auftretens bewirken, weil die Gefahr besteht, dass das eigene Verhalten überprüft und nicht autorisiert z. B. im Internet veröffentlicht wird. Bei einer ununterbrochenen Überwachung kann das Wissen, dass jede Bewegung und jede Geste von einer Kamera überwacht wird, mit weitreichenden psychologischen Auswirkungen verbunden sein. Der Einzelne fühlt sich ständig beobachtet und ist dadurch einem permanenten Überwachungsdruck ausgesetzt.
Mit dem Einsatz von Videoüberwachungsanlagen sind weitere Risiken verbunden. Es besteht die Gefahr, dass Aufzeichnungen missbraucht oder für fremde Zwecke genutzt werden. Elektronische Bilder können ohne Weiteres gespeichert, kopiert und unbegrenzt an eine Vielzahl von Empfängern in kürzester Zeit und ohne finanziellen Aufwand weitergeleitet werden. Umfassende räumliche und zeitliche Überwachungen ermöglichen die Erstellung von Bewegungs- und Verhaltensprofilen. Hinzu kommt, dass „intelligente“ Videoüberwachungssysteme keine reine Zukunftsmusik mehr sind. Technisch ist es beispielsweise möglich, gezielt einzelne Personen automatisiert über eine große räumliche Distanz zu verfolgen und mittels Bilderabgleich in Datenbanken eindeutig zu identifizieren. Machbar ist es auch, „auffällige“ oder vermeintlich nicht normale

Bewegungen und Verhaltensmuster herauszufiltern, anzuzeigen und gegebenenfalls Alarm auszulösen.
Diese Orientierungshilfe soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Sofern mit einer Kamera personenbezogene Daten erhoben werden, also z. B. Personen oder Kfz-Kennzeichen erkennbar sind, bedarf es nach dem so genannten Verbot mit Erlaubnisvorbehalt einer rechtlichen Grundlage für die Datenverarbeitung. Zu unterscheiden ist dabei zwischen der Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen (§ 6b des Bundesdatenschutzgesetzes [BDSG]), der Videoüberwachung von Beschäftigten (§ 32 Abs. 1 BDSG) und einer sonstigen Videoüberwachung in OH „Videoüberwachung durch nicht-öffentliche Stellen“ zugänglichen Räumen (§ 28 BDSG). Am Ende finden Sie einen Fragenkatalog, der Verantwortlichen und Datenschutzbeauftragten als Checkliste dienen kann.

2. Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen

Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welcher die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Nicht-öffentliche Stellen sind private Betreiber von Videotechnik, z. B. Unternehmen oder Privatpersonen.

2.1. *Anwendungsbereich und Voraussetzungen des § 6b Absatz 1 BDSG*

Im Folgenden wird beschrieben, wann diese Vorschrift Anwendung findet und welche Anforderungen sie an eine Videoüberwachungsanlage stellt.

2.1.1. Wann liegt eine Videoüberwachung vor?

§ 6b Absatz 1 BDSG definiert die Videoüberwachung als Beobachtung mit „optisch-elektronischen Einrichtungen“. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Dabei ist irre-

levant, ob sie über eine Zoomfunktion oder eine Schwenkvorrichtung verfügen, ob die Kamera stabil montiert oder frei beweglich ist. Auch der Einsatz von Webcams, Wildkameras, digitalen Fotoapparaten oder Mobiltelefonen mit integrierter Kamera ist grundsätzlich als Videoüberwachung anzusehen (s. hierzu auch Nr. 3.1.). Voraussetzung ist dabei jeweils die Erhebung personenbezogener Daten, das heißt, dass Personen auf den Aufnahmen erkennbar sein müssen oder sonst Rückschlüsse auf die Identität einer Person möglich sind.

Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Eine Videoüberwachung liegt bereits vor, sobald die Möglichkeit der Beobachtung gegeben ist, das bedeutet, dass unabhängig von einer möglichen Speicherung oder Aufzeichnung der Bilder schon bei bloßer Live-Beobachtung mittels optisch-elektronischer Einrichtung die Vorgaben des § 6b BDSG einzuhalten sind. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrundeliegt. Damit unterfällt beispielsweise das Anfertigen von Fotos in kurzen Zeitintervallen ebenfalls der Vorschrift. Die gezielte Beobachtung einzelner Personen wird nicht vorausgesetzt. Die Überwachungsmaßnahme setzt selbst dann bereits mit der Inbetriebnahme der Kameras ein, wenn die Geräte erst im Bedarfs- oder Alarmfall aufzeichnen.

Bei bloßen Kameraattrappen oder unzutreffenden Hinweisen auf eine Videoüberwachung gehen die Datenschutzaufsichtsbehörden der meisten Bundesländer davon aus, dass das Bundesdatenschutzgesetz nicht zur Anwendung kommt, da es sich bei Attrappen um keine optisch-elektronischen Einrichtungen handelt und deshalb keine personenbezogenen Daten erhoben werden. Allerdings erweckt auch das Anbringen von Kameraattrappen und unzutreffenden Hinweisen bei Personen, die diese zur Kenntnis nehmen, regelmäßig den Eindruck, dass sie tatsächlich videoüberwacht werden. Da die fehlende Funktionsfähigkeit der Kamera von außen nicht erkennbar ist, kann ein Überwachungsdruck hervorgerufen werden[1)], der eine Beeinträchtigung des Persönlichkeitsrechts darstellen und damit zivilrechtliche Abwehransprüche auslösen kann. Diese müssen notfalls im

[1)] LG Bonn, Urteil vom 16. November 2004 - 8 S 139/04; AG Lichtenberg, Beschluss vom 24.01.2008 - 10 C 156/07.

Klageweg durchgesetzt werden. Ob darüber hinaus ein aufsichtsbehördliches Einschreiten gegen eine Attrappe in Betracht kommt, differiert danach, ob die örtlich zuständige Aufsichtsbehörde hierfür auch eine sachliche Zuständigkeit anerkennt. Dies erfahren Betroffene ggf. auf Nachfrage.

2.1.2. *Was ist ein öffentlich zugänglicher Raum?*

Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Ein öffentlicher Raum liegt auch dann vor, wenn für den Zugang besondere allgemeine Voraussetzungen, wie etwa ein bestimmtes Mindestalter, erfüllt sein müssen, ein Eintrittspreis zu entrichten ist oder die Öffnung nur zu bestimmten Zeiten erfolgt. Darauf, ob der überwachte Bereich Privateigentum ist oder nicht, kommt es nicht an.
Zu den öffentlich zugänglichen Räumen gehören neben öffentlichen Verkehrsflächen beispielsweise Ausstellungsräume eines Museums, Verkaufsräume, Schalterhallen, Tankstellen, Biergärten, öffentliche Parkhäuser, Gasträume von Gaststätten oder Hotelfoyers.
Nicht öffentlich zugänglich sind demgegenüber Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Hierzu gehören etwa Büros oder Produktionsbereiche ohne Publikumsverkehr. Entscheidend ist hierbei, dass die Nicht-Öffentlichkeit durch Verbotsschilder oder den Kontext der Umgebung erkennbar ist. Die eigene private Wohnung zählt z. B. zu den nicht öffentlich zugänglichen Räumen. Zu beachten ist allerdings, dass die Einordnung als nicht öffentlich zugänglicher Raum vom Einzelfall abhängig ist. Das Treppenhaus eines Wohnhauses ist beispielsweise grundsätzlich ein nicht öffentlich zugänglicher Raum. Befindet sich im Haus allerdings eine Arztpraxis oder eine Anwaltskanzlei mit offenem Publikumsverkehr, dann ist dies bereits ausreichend, um das Treppenhaus während der Geschäftszeiten als öffentlich zugänglich einzuordnen. Eine Videoüberwachung nicht-öffentlich zugänglicher Räume kann unter Umständen nach § 28 BDSG zu beurteilen sein (siehe unten Nr. 5.).
Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche

Verkehrsraum in der Umgebung und die sich dort befindlichen Personen erfasst werden. Bei einem Nachbargrundstück handelt es sich nicht um einen öffentlichen Raum; dessen Beobachtung ist daher nicht von § 6b BDSG erfasst. Allerdings greift eine Überwachung von Nachbargrundstücken in die Persönlichkeitsrechte des Nachbarn ein. Dieser kann sich daher auf zivilrechtlichem Weg mittels Abwehr- und Unterlassungsansprüchen gegen die Videoüberwachung zur Wehr setzen (zur Videoüberwachung im Nachbarschaftsverhältnis vergleiche unten Nr. 5).

2.1.3. *Zulässigkeit einer Videoüberwachung öffentlich zugänglicher Räume*

Nach § 6b Absatz 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (2.1.3.1.) erforderlich ist (2.1.3.2.) und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen (2.1.3.3.).

2.1.3.1. Zweck der Videoüberwachung

Bevor eine Videoüberwachung installiert wird, ist zu konkretisieren, welches Ziel damit erreicht werden soll. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren. Auch die Beweissicherung durch die Aufzeichnung kann ein solches berechtigtes Interesse darstellen.
In bestimmten Fällen kann auch eine abstrakte Gefährdungslage ausreichend sein, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die

wertvolle Ware verkaufen (z. B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind (z. B. Tankstellen).
Darüber hinaus ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret anzugeben.

2.1.3.2. Geeignetheit und Erforderlichkeit der Videoüberwachung

Vor dem Einsatz eines Videoüberwachungssystems ist zu überprüfen, ob es tatsächlich für den festgelegten Zweck geeignet und erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann.
Vor der Installation einer Videoüberwachungsanlage muss man sich deshalb mit zumutbaren alternativen Methoden auseinandersetzen, die in das Persönlichkeitsrecht des Einzelnen weniger eingreifen. Eine Umzäunung, regelmäßige Kontrollgänge von Bewachungspersonal, der Einsatz eines Pförtners, der Einbau von Sicherheitsschlössern oder von einbruchsicheren Fenstern und Türen können beispielsweise ebenfalls einen wirksamen Schutz gegen Einbruch und Diebstahl bieten. Das Auftragen von spezieller Oberflächenbeschichtung kann Schutz vor Beschädigungen durch Graffiti bieten.
Des Weiteren muss vor Inbetriebnahme einer Kameraanlage eine Überprüfung dahingehend erfolgen, an welchen Orten und zu welchen Zeiten eine Überwachung unbedingt notwendig erscheint. Häufig kann eine Überwachung in den Nachtstunden oder außerhalb der Geschäftszeiten ausreichend sein.
Im Rahmen der Erforderlichkeit ist ferner zu untersuchen, ob eine reine Beobachtung im Wege des Live-Monitorings ausreichend ist, oder ob es zum Erreichen des Überwachungszwecks einer (regelmäßig eingriffsintensiveren) Aufzeichnung bedarf. In diesem Zusammenhang ist zu betonen, dass eine reine Aufzeichnung (Black-Box) für präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. Sicherheitspersonal unmittelbar eingreifen kann. Das

bedeutet, dass eine Videoaufzeichnung zur Verhinderung von Unfällen oder Straftaten nicht geeignet ist.
Unter dem Aspekt der Datenvermeidung und Datensparsamkeit ist weiterhin zu prüfen, ob durch den Einsatz spezieller Technik bestimmte Bereiche des Aufnahmefeldes ausgeblendet oder die Gesichter der sich in diesen Bereichen aufhaltenden Personen „verschleiert“ werden können.

2.1.3.3. Beachtung der schutzwürdigen Interessen des Betroffenen

Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Maßstab der Bewertung ist das informationelle Selbstbestimmungsrecht als besondere Ausprägung des Persönlichkeitsrechts auf der einen und der Schutz des Eigentums oder der körperlichen Unversehrtheit auf der anderen Seite. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist häufig die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art der erfassten Informationen (Informationsgehalt), Umfang der erfassten Informationen (Informationsdichte, zeitliches und räumliches Ausmaß), den betroffenen Personenkreis, die Interessenlage der betroffenen Personengruppen, das Vorhandensein von Ausweichmöglichkeiten sowie Art und Umfang der Verwertung der erhobenen Daten bestimmt. In den Fällen, in denen die Videoaufnahmen nicht nur auf einen Monitor übertragen, sondern auch aufgezeichnet werden sollen, ist eine diesbezügliche Abwägung mit den schutzwürdigen Interessen der Betroffenen erneut vorzunehmen.
Grundsätzlich unzulässig sind Beobachtungen, die die Intimsphäre der Menschen verletzen, etwa die Überwachung von Toiletten, Saunas, Duschen oder Umkleidekabinen. Die schutzwürdigen Interessen überwiegen außerdem häufig dort, wo die Entfaltung der Persönlichkeit im Vordergrund steht, beispielsweise in Restaurants, Erlebnis- und Erholungsparks, wo Leute kommunizieren, essen und trinken oder sich erholen.

Auch eine permanente Überwachung, der eine betroffene Person nicht ausweichen kann, stellt einen gravierenderen Eingriff dar als eine Beobachtung, die lediglich zeitweise erfolgt und nur Teilbereiche des Raumes erfasst. Dies ist zum Beispiel bei der dauerhaften Überwachung von öffentlichen Zufahrten und Eingängen zu Mehrfamilienhäusern relevant, da die Bewohner auf die Nutzung des überwachten Bereichs angewiesen sind.
Grundsätzlich gilt, je mehr persönliche Informationen aufgrund der Überwachung erhoben werden, desto intensiver ist der Eingriff in die Grundrechte und in die schutzwürdigen Interessen der Betroffenen.
Ermöglicht die Qualität der Aufnahme keine Personenbeziehbarkeit, sind schutzwürdige Interessen Betroffener schon deshalb nicht verletzt, weil es an einer Datenerhebung im Sinne des § 3 Absatz 3 BDSG fehlt.

2.2. Einzelne Maßnahmen vor Einrichtung einer Videoüberwachung

Vor dem Einsatz einer Videoüberwachungsanlage gilt es, im Vorhinein einige Maßnahmen und Voraussetzungen nach dem Bundesdatenschutzgesetz durchzuführen und einzuhalten.

2.2.1. *Verfahrensverzeichnis, Vorabkontrolle, Sicherungspflichten*

Vor Beginn der Videoüberwachung ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme (vergleiche Nr. 2.1.3.1.) schriftlich festzulegen. Zudem sind technische und organisatorische Maßnahmen zu treffen (§ 9 BDSG), um die Sicherheit der Daten zu gewährleisten.
Vor der Inbetriebnahme einer Videoüberwachung ist eine Vorabkontrolle nach § 4d Absatz 5 BDSG erforderlich, wenn bei dem Einsatz der Videotechnik von besonderen Risiken für die Rechte und Freiheiten der Betroffenen auszugehen ist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Der betriebliche Datenschutzbeauftragte (bDSB) hat gemäß § 4d Absatz 6 BDSG die Vorabkontrolle durchzuführen und das Ergebnis sowie die Begründung schriftlich zu dokumentieren.

Unabhängig von der Durchführung einer Vorabkontrolle ergibt sich das Erfordernis der vorherigen Zweckbestimmung aus § 6b Absatz 1 Nr. 3 BDSG, wenn die Videoüberwachung zur Wahrnehmung berechtigter Interessen erfolgt. Darüber hinaus ist für Verfahren, die automatisiert Daten verarbeiten, eine Verfahrensübersicht zu erstellen (vergleiche § 4g Absatz 2 und 2a BDSG). Eine Videoüberwachung ist jedenfalls dann, wenn sie mittels digitaler Technik erfolgt, als automatisierte Verarbeitung zu qualifizieren. Welche Angaben in diese Übersicht aufgenommen werden müssen, zählt § 4e Satz 1 BDSG verbindlich und abschließend auf. Der dort geforderten allgemeinen Beschreibung der technisch-organisatorischen Maßnahmen zum Schutz der Daten kommt bei der Videoüberwachung besondere Bedeutung zu. Die Videobilddaten unterliegen wegen der sich aus einer unsachgemäßen Handhabung möglicherweise für den Betroffenen ergebenden Beeinträchtigungen entsprechend hohen Schutzkontrollen sowohl hinsichtlich des Zutritts, Zugangs und Zugriffs, aber auch der Weitergabe an Strafverfolgungsbehörden im Deliktfall. In der Verfahrensübersicht sind darüber hinaus die zugriffsberechtigten Personen zu benennen.
Die Verfahrensübersicht ist von der verantwortlichen Stelle zu erstellen und dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Dieser muss die Inhalte der Verfahrensübersicht bis auf die Angaben zu dem Bereich des Datensicherheitsmanagements auf Antrag jedermann zugänglich machen. Dieses öffentlich zugängliche Papier nennt man Verfahrens- oder auch „Jedermannverzeichnis“. Sofern keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, fällt dem Leiter der nicht-öffentlichen Stelle die Pflicht zu, die Erfüllung dieser Aufgaben des betrieblichen Datenschutzbeauftragten in anderer Weise sicherzustellen.

2.2.2. *Hinweispflicht*

Nach § 6b Absatz 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage

versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

2.3. Durchführung einer zulässigen Videoüberwachung

2.3.1. *Speicherdauer*

Gemäß § 6b Absatz 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ist es beispielsweise an einer Tankstelle zu keinem Überfall oder Diebstahl gekommen, werden Videoaufzeichnungen für Beweiszwecke nicht mehr benötigt und sind daher zu löschen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können.[2)] Das bedeutet, dass Videoaufzeichnungen grundsätzlich nach 48 Stunden zu löschen sind. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, etwa wenn an Wochenenden und Feiertagen kein Geschäftsbetrieb erfolgt. Da sich die gesetzliche Speicherdauer am Aufzeichnungszweck orientiert, kann der Zeitpunkt der Löschpflicht je nach Einzelfall variieren.
Dem Löschungsgebot wird am wirksamsten durch eine automatisierte periodische Löschung, z. B. durch Selbstüberschreiben zurückliegender Aufnahmen, entsprochen.

2.3.2. *Unterrichtungspflicht*

[2)] Vgl. die Gesetzesbegründung, BT-Drs. 14/5793, S. 63.

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Absatz 4 BDSG). Zweck dieser Regelung ist es, Transparenz zu schaffen und der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Eine Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen. Die Notwendigkeit einer Benachrichtigung besteht erst bei einer tatsächlichen Zuordnung, allein die Möglichkeit dazu macht eine Benachrichtigung noch nicht erforderlich. Die Benachrichtigung hat bei der erstmaligen Zuordnung zu erfolgen.

2.3.3. *Tonaufzeichnungen*

Für solche Überwachungsmaßnahmen ist im Strafgesetzbuch (StGB) mit § 201 (Verletzung der Vertraulichkeit des Wortes) eine Regelung enthalten, die es unter Strafandrohung verbietet, das nicht-öffentlich gesprochene Wort aufzuzeichnen oder abzuhören. Sofern eine Videoüberwachungskamera daher über eine Audiofunktion verfügt, ist diese irreversibel zu deaktivieren.

2.3.4. *Überprüfung der Rechtmäßigkeitsvoraussetzungen*

Der Betreiber einer Videoüberwachungsanlage ist verpflichtet, die rechtlichen Voraussetzungen für den Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Geeignetheit und Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kamera in Betrieb war, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachung nicht weiter betrieben werden. Dies kann auch Teilbereiche einer Überwachung betreffen. Das Ergebnis der Überprüfung sollte schriftlich dokumentiert werden.

3. Besondere Fallkonstellationen

3.1. *Webcams*

Webcams ermöglichen es, Live-Aufnahmen ins Internet einzustellen und damit einer unbestimmten Zahl von Personen weltweit zugänglich zu machen. Problematisch ist dabei, dass Persönlichkeitsrechtsverletzungen bei einer Live-Übertragung nicht mehr rückgängig gemacht werden können. Für zufällig von der Kamera erfasste Personen besteht daher ein großes Risiko, das durch die steigende Qualität und die einfache Möglichkeit der technischen Vervielfältigung und Bearbeitung der Aufnahmen noch erhöht wird. Der Einsatz einer Webcam ist nur dann datenschutzrechtlich unbedenklich, sofern auf den aufgenommenen Bildern – etwa aufgrund der Kamerapositionierung, fehlender Zoom-Möglichkeiten oder niedriger Auflösung – Personen oder Kfz-Kennzeichen nicht erkannt werden können.

3.2. *Videoüberwachung in der Gastronomie*

Die Videoüberwachung des Gastraumes einer Gaststätte[3)] ist nach § 6b BDSG im Regelfall datenschutzrechtlich unzulässig. Jedenfalls die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind Kundenbereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und daher nicht mit Videokameras überwacht werden dürfen.[4)] Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechtigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann.

[3)] Gemeint ist die Gaststätte im Sinne des Gaststättengesetzes (GastG), d. h. ein Betrieb, in welchem Getränke und/oder Speisen zum Verzehr an Ort und Stelle verabreicht werden und der jedermann oder bestimmten Personenkreisen zugänglich ist (§ 1 GastG). Unter den Gaststättenbegriff fallen somit auch Cafés, Imbisslokale, Schnellrestaurants etc.

[4)] Vgl. AG Hamburg, Urteil vom 22.04.2008 – 4 C 134/08.

Gleiches gilt für Café- und Gastrobereiche in Bäckereien, Tankstellen, Hotels etc.

4. *Videoüberwachung von Beschäftigten*

Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden, zum Beispiel in Verkaufsräumen im Einzelhandel. In solchen Fällen ist nicht nur die Persönlichkeitssphäre der Kunden betroffen, sondern es kommt auch zu einer Überwachung der dort tätigen Beschäftigten. Für solche Bereiche, in denen die Wahrscheinlichkeit von Straftaten zu einem geschäftstypischen Risiko gehört und die Erfassung der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, überwiegt in Einzelfällen das berechtigte Interesse des Arbeitgebers, Straftaten vorzubeugen. Dennoch ist bei der Installation der Videoüberwachung das Einrichten von so genannten Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich Beschäftigte länger aufhalten, erforderlich. Je weniger Rückzugsmöglichkeiten den Beschäftigten in nicht überwachten Bereichen zur Verfügung stehen, desto eher überwiegen deren schutzwürdige Interessen.
Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten der Beschäftigten durch eine Videoanlage kann in der Regel nicht auf § 32 Absatz 1 Satz 1 BDSG gestützt werden. Denkbar sind offene Überwachungsmaßnahmen danach jedoch insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Jedoch ist in diesem Zusammenhang der Erfassungsbereich auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte soweit wie möglich auszublenden. Eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen Dienstablauf zu gewährleisten, ist nicht gerechtfertigt.
Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nach § 32 Absatz 1 Satz 2 BDSG nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforder-

lich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.
Eine Videoüberwachung, die in nicht öffentlich zugänglichen Räumen stattfindet und nicht in Zusammenhang mit dem Beschäftigungsverhältnis steht, ist an den Voraussetzungen des § 28 Absatz 1 Satz 1 Nr. 2 BDSG zu messen. Der Einsatz von Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. So können ausnahmsweise auch Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Fokus der Überwachung steht und nicht permanent erfasst wird, z. B. der nächtliche Wachmann, der die zum Zweck der Verhinderung und Aufklärung von Diebstählen videoüberwachten Lagerräume kontrolliert, in denen wertvolle Ware aufbewahrt wird. Aber auch hier ist zuvor zu prüfen, ob weniger einschneidende Mittel in Betracht kommen.
Für die Bewertung der Zulässigkeit einer solchen Maßnahme ist ergänzend die Rechtsprechung des Bundesarbeitsgerichts[5)] zugrundezulegen. In wenigen Ausnahmefällen kann danach die Überwachung von Beschäftigten mittels Kameras durch den Arbeitgeber dann zulässig sein, wenn sie offen erfolgt, die Beschäftigten also wissen, dass ihr Arbeitsplatz videoüberwacht wird. Entscheidend ist, ob der Arbeitgeber ein berechtigtes Interesse an den Kameraaufnahmen hat, etwa um Diebstählen oder Vandalismus durch sein Personal vorzubeugen. Hat er ein solches, berechtigt ihn dieses jedoch nicht ohne Weiteres zur Überwachung. Vielmehr muss sein Interesse mit den schutzwürdigen Interessen des Beschäftigten, nicht in seinem Persönlichkeitsrecht verletzt zu werden, abgewogen werden. Das Persönlichkeitsrecht schützt den Beschäftigten vor einer lückenlosen Überwachung am Arbeitsplatz durch Videoaufnahmen, die ihn einem ständigen Überwachungsdruck aussetzen, dem er sich nicht entziehen kann. Deswegen überwiegt das Beschäftigteninteresse, von einer derartigen Dauerüberwachung verschont zu bleiben, wenn der Arbeitgeber mit der Überwachung nur befürchteten Verfehlungen

[5)] Vgl. insb. BAG, Urteil vom 27.03.2003 – 2 AZR 51/02; Beschluss vom 29.06.2004 – 1 ABR 21/03; Beschluss vom 14.12.2004 – 1 ABR 34/03; Beschluss vom 26.08.2008 – 1 ABR 16/07; Urteil vom 21.06.2012 – 2 AZR 153/11.

seiner Beschäftigten präventiv begegnen will, ohne dass hierfür konkrete Anhaltspunkte bestehen.
In der Abwägung wird auch gewichtet, ob den Beschäftigten überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich verbleibt. Zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz sind Kameras keinesfalls erlaubt. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind ebenfalls von der Überwachung auszunehmen.
Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die Videoüberwachung praktisch die einzig verbleibende Möglichkeit zur Aufklärung oder zur Verhinderung des Missstandes darstellt und insbesondere im Hinblick auf den angerichteten oder zu verhindernden Schaden nicht unverhältnismäßig ist.
Kann die Datenerhebung und -verarbeitung im Beschäftigungsverhältnis nicht auf eine Rechtsgrundlage gestützt werden, ist die Videoüberwachung wegen § 4 Absatz 1 BDSG (Verbot mit Erlaubnisvorbehalt) unzulässig. Eine etwaige arbeitgeberseitig eingeholte Einwilligung des Beschäftigten ist irrelevant, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4a Absatz 1 Satz 1 BDSG mangelt.
Soweit die Videoüberwachung den gesetzlichen Vorgaben entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung näher geregelt werden. Die Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sollten näher beschrieben werden. Dazu gehören insbesondere

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Zweckbindung
- Datenvermeidung und Datensparsamkeit
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Empfänger der Daten
- Rechte der Betroffenen
- Löschfristen
- Technische und organisatorische Maßnahmen wie beispielsweise das Berechtigungskonzept

Soweit ein Betriebsrat nicht existiert, sollte der Arbeitgeber entsprechende Dienstanweisungen erstellen.

Zulässige Verfahren zur Videoüberwachung ermöglichen in der Regel eine Bewertung der Persönlichkeit der betroffenen Beschäftigten einschließlich ihrer Fähigkeiten, ihrer Leistungen und ihres Verhaltens. Daher ist nach § 4d Absatz 5 Satz 2 Nr. 2 BDSG regelmäßig eine Vorabkontrolle durchzuführen (vergleiche oben Nr. 2.2.1.).

5. *Sonstige Videoüberwachung durch nicht-öffentliche Stellen, insbes. Videoüberwachung durch Nachbarn oder Vermieter*

Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kameras zu unterscheiden. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen endet. Wer außer seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mitüberwacht werden.
Sofern sich die Videoüberwachung auf das Grundstück des Nachbarn erstreckt, ohne dass eine öffentlich zugängliche Fläche betroffen ist, ist die Anwendbarkeit des Bundesdatenschutzgesetzes zumeist deshalb zu verneinen, da es sich um eine persönliche bzw. familiäre Tätigkeit im Sinne des § 1 Absatz 2 Nr. 3 BDSG handelt, welche vom Regelungsbereich des Bundesdatenschutzgesetzes ausgenommen ist. Dies hat zur Folge, dass die Anlage nicht der Kontrolle der Datenschutzaufsichtsbehörden unterliegt. Videoüberwachten Nachbarn stehen jedoch unabhängig davon unter Umständen zivilrechtliche Unterlassungs- und Abwehransprüche zu. Diese müssten auf dem Zivilrechtsweg gegebenenfalls unter Einschaltung eines Rechtsanwalts geltend gemacht werden. Darüber hinaus kann das Beobachten fremder Grundstücke mit einer Videoanlage strafrechtliche Konsequenzen haben, wenn damit der höchstpersönliche

Lebensbereich der beobachteten Person verletzt wird (vergleiche § 201a Strafgesetzbuch).
Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b BDSG richtet (vergleiche oben Nr. 2.1.2.). In diesen Fällen greift § 28 BDSG, wonach ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. Außerdem besteht in diesen Fällen ebenfalls die Möglichkeit, mit zivilrechtlichen Unterlassungs- und Abwehransprüchen gegen einen etwaigen Eingriff in das Persönlichkeitsrecht vorzugehen. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum und im Fahrstuhl selbst, einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. In der hierzu ergangenen zivilrechtlichen Rechtsprechung[6)] besteht Einigkeit darüber, dass eine Rundumüberwachung des sozialen Lebens nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Schmierereien, Verschmutzungen oder einmaligen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

[6)] Vgl. beispielsweise LG Berlin, Urteil vom 23.05.2005 – 62 S 37/05; KG Berlin, Beschluss vom 04.08.2008 – 8 U 83/08; AG München, Urteil vom 16.10.2009 – 423 C 34037/08.

6. Checkliste für den Betreiber einer Videoüberwachung öffentlich zugänglicher Räume

Planen Sie die Installation von Videokameras oder betreiben Sie bereits eine Videoüberwachungsanlage? Folgende Fragen sollten Sie für eine zulässige Überwachungsmaßnahme beantworten können:

1. Welche Bereiche sollen überwacht werden?
   - öffentlich zugänglicher Raum (z. B. Kundenbereiche);
   - Mitarbeiterräume;
   - öffentliche Flächen (z. B. Gehwege)
2. Dient die Videoüberwachung der
   - Wahrung des Hausrechts
   oder
   - Wahrung eines anderen berechtigten Interesses (Zweck)?
   Wenn ja, welchem?
   Besteht eine Gefährdungslage und auf welche Tatsachen, z. B. Vorkommnisse in der Vergangenheit, gründet sich diese?
3. Wurde der Zweck der Videoüberwachung schriftlich festgelegt?
4. Warum ist die Videoüberwachung geeignet, den festgelegten Zweck zu erreichen?
5. Warum ist die Videoüberwachung erforderlich und warum gibt es keine milderen Mittel, die für das Persönlichkeitsrecht der Betroffenen weniger einschneidend sind?
6. Welche schutzwürdigen Interessen der Betroffenen haben Sie mit welchem Ergebnis in die Interessenabwägung einbezogen?
7. Ist eine Beobachtung der Bilder auf einem Monitor ohne Aufzeichnung der Bilddaten ausreichend? Wenn nein, warum nicht?
8. Sofern aufgezeichnet wird, wann werden die Aufnahmen gelöscht? Wenn das Löschen nicht innerhalb von 48 Stunden erfolgt, begründen Sie bitte das spätere Löschen.
9. Zu welchen Zeiten erfolgt die Videoüberwachung und wer hält sich üblicherweise zu dieser Zeit im überwachten Bereich auf?
10. Wenn eine Videoüberwachung rund um die Uhr erfolgt, warum halten Sie sie für erforderlich bzw. warum kann sie nicht

zeitlich eingeschränkt werden, z. B. auf außerhalb der Geschäftszeiten oder die Nachtstunden?

11. Werden bestimmte Bereiche der Überwachung ausgeblendet oder verpixelt? Wenn nein, warum nicht?
12. Über welche Möglichkeiten verfügt die Videokamera und welche hiervon sind für die Überwachung nicht erforderlich und ggfM. zu deaktivieren?
    - hinsichtlich der Ausrichtung, z. B. schwenkbar oder variabel, Domekamera
    - bezüglich der Funktionalität, z. B. Zoomobjektive, Funkkameras, Audiofunktion
13. Wurde geprüft, ob eine Vorabkontrolle erforderlich ist und wurde sie ggf. durch die bzw. den betrieblichen Datenschutzbeauftragten durchgeführt? Wenn nein, warum ist eine Vorabkontrolle nicht erforderlich?
14. Wird auf die Videoüberwachung so hingewiesen, dass der Betroffene vor Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann?
15. Wird in dem Hinweis die verantwortliche Stelle genannt?
16. Unter welchen Voraussetzungen wird Einsicht in die Aufnahmen genommen?
    Durch wen?
    Ist die Protokollierung der Einsichtnahme sichergestellt?
    Wurden die zugriffsberechtigten Personen auf das Datengeheimnis verpflichtet?
17. Wurden die technisch-organisatorischen Maßnahmen zum Schutz der Daten nach § 9 BDSG (und der Anlage hierzu) getroffen?
18. Gibt es im Unternehmen einen Betriebsrat und wurde mit diesem eine Betriebsvereinbarung zur Videoüberwachung getroffen?

Rein vorsorglich weisen wir darauf hin, dass eine Beschäftigung mit diesen Fragen nicht automatisch zur Zulässigkeit der Videoüberwachungsmaßnahme führt.

Haben Sie zu dem Betrieb der Videoüberwachungsanlage konkrete Fragen, können Sie sich gerne an die für Sie zuständige Datenschutzaufsichtsbehörde wenden. Maßgeblich ist grundsätzlich der Sitz des Betreibers. Eine Übersicht über die Kontaktdaten erhalten

Sie beispielsweise unter http://www.baden-wuerttemberg.datenschutz.de/die-aufsichtsbehorden-der-lander/.

Anlage 4

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 25./26. Februar 2014)

Unzulässigkeit von Videoüberwachung aus Fahrzeugen
(sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.
Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.
Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder

sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

Anlage 5

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 25./26. Februar 2014)

Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.
Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.
Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.
Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.
Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.
Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in **eigener** Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.
Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und orga-

nisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.
Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne Weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.
Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

Anlage 6

Gemeinsame Position
der
Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)
und der
Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten
(Mai 2014)

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von **Fernsehangeboten** muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als **Telemedien** den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.
   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
   - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass

dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Anlage 7

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 16. Juni 2014)

Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter

Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich.

Die Orientierungshilfe ist abrufbar unter folgendem Link:

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/OHApps.pdf?__blob=publicationFile&v=3

Anlage 8

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 15./16. September 2015)

Nutzung von Kameradrohnen durch Private

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne Weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr.1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu

betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201 a Strafgesetzbuch [StGB]), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

Anlage 9

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 15./16. September 2015)

Videoüberwachung in öffentlichen Verkehrsmitteln

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z. B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z. B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw. dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu

fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z. B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwachung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o. Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frage ankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und

Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken – wie beispielsweise dem länderübergreifenden Bahnbetrieb – eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z. B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z. B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahme-

fällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z. B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetrieb-

nahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens "Videoüberwachung" mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vergleiche § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit

der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art

der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vergleiche Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z. B. pauschal eine möglichst umfassende Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich z. B. nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter be-

trieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

Anlage 10

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis, 27. Januar 2014)

Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten"

Einleitung

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. An der Beantwortung der Fragen muss der Vermieter ein berechtigtes Interesse haben oder es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss das Recht des Mietinteressenten auf informationelle Selbstbestimmung Beachtung finden.

Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft ist nicht als das richtige Mittel zur Datenerhebung anzusehen. Eine wirksame Einwilligung erfordert nach § 4a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Dem Mietinteressenten wird dabei suggeriert, er habe bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht. Wird der Abschluss des Mietvertrags von der Erhebung bestimmter Angaben beim Mietinteressenten abhängig gemacht, fehlt diese Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommt.
Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden: (a) dem Besichtigungstermin, (b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und (c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Die Zulässigkeit der Erhebung einer Selbstauskunft richtet sich im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht dann ein vorver-

tragliches Schuldverhältnis zum künftigen Vermieter, so dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Steht dem Vermieter für die Datenerhebung eine gesetzliche Grundlage nach § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG zur Verfügung, so kommt es auf die Anforderungen nach § 4a Abs. 1 Satz 1 BDSG nicht an bzw. ein Rückgriff auf das Konstrukt der Einwilligung wäre auch falsch, denn für den Mietinteressenten würde wiederum der Eindruck entstehen, dass die Offenbarung der Informationen seinem Wahlrecht unterliegt. Bei der Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG kommt es dann im Rahmen der Erforderlichkeitsprüfung darauf an, ob von Seiten des Interessenten aus Offenbarungspflichten bestehen bzw. ob von Vermieterseite aus zulässige Fragen gestellt werden. Unzulässige Fragen müssen demnach nicht beantwortet werden (Blank, in: Schmidt-Futterer, Kommentar zum Mietrecht, 11. Auflage 2013, § 543, Rn. 204). Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen des Mietinteressenten am Ausschluss der Datenerhebung bestehen.

Die folgende Darstellung ist nicht im Sinne einer abschließenden Aufzählung zu verstehen:

a) Besichtigungstermin
Strebt der Mietinteressent nur eine Besichtigung der Räumlichkeiten an, so wäre es etwa nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen.
Erfragt werden dürfen:

aa) Angaben zur Identifikation
Hierzu zählen Name, Vorname und Anschrift. Der Vermieter wäre auch befugt, im Falle der Besichtigung allein durch den Mietinteressenten die Angaben durch Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.

bb) Angaben aus Wohnberechtigungsschein
Der künftige Vermieter darf nach § 27 Abs. 1 Wohnraumförderungsgesetz (WoFG) eine Wohnung, die im Rahmen eines Pro-

gramms zur sozialen Wohnraumförderung errichtet wurde, nur einem Wohnungssuchenden zum Gebrauch überlassen, wenn dieser ihm vorher seine Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweist. Möchte der Mietinteressent eine solche Wohnung besichtigen, sind Angaben zum Vorliegen eines Wohnberechtigungsscheins sowie zur genehmigten Wohnfläche und Anzahl der Wohnräume erforderlich, da nur in diesem Fall ein Besichtigungstermin sinnvoll ist. Eine Kopie des Wohnberechtigungsscheins darf erst nach der Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen, erfolgen, da die in dem Formular aufgeführten Angaben zu den Namen und Vornamen der im Haushalt des Mietinteressenten befindlichen Personen im Besichtigungstermin nicht erforderlich sind.

cc) Angaben zu Haustieren

Fragen des Vermieters nach dem beabsichtigten Einbringen von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Entsprechende Fragen sind zulässig, soweit dies nicht Kleintiere betrifft (z. B. Zierfische, Mäuse, Hamster).

b) Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen

aa) Familienstand und Angaben zu den im Haushalt lebenden Personen

Angaben zum Familienstand des Mietinteressenten werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein aus dieser Zwecksetzung heraus ist kein berechtigtes Vermieterinteresse gegeben, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen. Soweit nur ein Ehegatte den Wohn-Mietvertrag unterzeichnen möchte und im Hinblick auf die äußere Gestaltung des Mietvertrags und die mündlichen Absprachen nicht davon ausgegangen werden kann, dass auch der andere Ehegatte Mietvertragspartei wird, greift keine gesamtschuldnerische Haftung ein. Schließlich ginge auch das Argument ins Leere, von Vermieterseite aus einer möglichen Gebrauchsüberlassung an Dritte zuvorzukommen, denn nach § 553 Abs. 1 BGB hätte der Mieter im Regelfall ein berechtigtes Interesse daran, dem Ehegatten den Wohnraum zur Nutzung zu überlassen.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben dürfen zu diesen Personen nicht eingeholt werden, es sei denn, diese möchten Mietvertragspartner sein.

bb) Eröffnetes Insolvenzverfahren, Angabe einer Vermögensauskunft, Räumungstitel wegen Mietzinsrückständen

Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05).

Bei der Angabe einer Vermögensauskunft (§ 802c Abs. 3 ZPO) sind Mietzinsansprüche des Vermieters nicht in gleicher Weise gefährdet (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05). Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften besteht, hängt u.a. davon ab, nach welchem Zeitraum gefragt wird. Ferner ist zu berücksichtigen, dass gemäß § 882f Satz 1 Nr. 4 ZPO eine Einsicht in das Schuldnerverzeichnis unter bestimmten Voraussetzungen möglich ist und zum Inhalt eines solchen Verzeichnisses auch Eintragungsanordnungen nach § 882c ZPO zählen. Nach § 882f Satz 1 Nr. 4 ZPO ist die Einsicht in das Schuldnerverzeichnis jedem gestattet, der darlegt, Angaben nach § 882b ZPO zu benötigen, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Im Hinblick auf den erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung des Mietinteressenten ist bei der Anwendung von § 882f Satz 1 Nr. 4 ZPO vor allem der Verhältnismäßigkeitsgrundsatz zu beachten. Ferner muss den wirtschaftlichen Nachteilen bedeutsames Gewicht zukommen (Utermark, in: Vorwerk/Wolf, Beck`scher Online-Kommentar ZPO, 2013, § 882f, Rn 7). An die Zulässigkeit einer Datenerhebung beim Vollstreckungsgericht nach § 882f Satz 1 Nr. 4 ZPO sind ähnlich hohe Anforderungen zu stellen, wie im Rahmen einer Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG beim Mietinteressenten.

Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnis mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht (AG Wolfsburg, Urteil v. 09.08.2000, Az.: 22 C 498/99). Fragen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchgeführt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, werden als zulässig angesehen (LG Wuppertal, Urteil v. 17.11.1998, Az.: 16 S 149/98).

cc) Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit

Nach § 19 Abs. 1 und 3 AGG ist bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum eine unterschiedliche Behandlung im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zulässig. Es fehlt regelmäßig an der Erforderlichkeit der Datenerhebung, da die Anforderungen nach denn §§ 19, 20 AGG kaum erfüllt sein werden. Hierfür müsste zur Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zunächst ein tragfähiges Vermietungskonzept vorliegen. Das Konzept muss auch zur Prüfung sachlicher Gründe (vergleiche etwa § 20 Abs. 1 Nr. 4 AGG) Auskunft geben, die eine Ungleichbehandlung rechtfertigen und folglich zur Entschärfung von Konflikten beitragen können. Eine pauschale Abfrage der Angaben ist daher unzulässig.

dd) Vorstrafen und strafrechtliche Ermittlungsverfahren

Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Berücksichtigt werden muss zum einen, dass bestimmte Strafen nicht in ein polizeiliches Führungszeugnis aufzunehmen sind, § 32 Abs. 2 BZRG, und sich schon deshalb keine darüber hinausgehenden Mitteilungspflichten gegenüber einem Vermieter ergeben können. Weiterhin hat die Rechtsprechung

eine Offenbarung von Vorstrafen bisher nur im Zusammenhang mit der Begründung von Arbeitsverhältnissen als zulässig angesehen, wenn ein klarer Bezug zu einer entsprechenden Tätigkeit besteht, wie etwa das Fragen nach Vermögensdelikten bei einer Beschäftigung im Kassenbereich eines Kreditinstituts. Dabei steht die Frage nach der Geeignetheit eines Bewerbers im Mittelpunkt. Bei der Anbahnung von Mietverhältnissen besteht grundsätzlich keine vergleichbare Gefährdungslage, da hier die Frage nach der Bonität des Mietinteressenten von zentraler Bedeutung ist. Gegen die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren spricht schon die verfassungsrechtlich und auch in Art. 6 Abs. 2 EMRK verankerte Unschuldsvermutung.

ee) Heiratsabsichten, Schwangerschaften, Kinderwünsche

Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und Kinderwünschen zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig. Eine Aufnahme von Kindern und Ehegatten in der Wohnung wäre für den Mietinteressenten schon nicht erlaubnispflichtig im Sinne von § 553 Abs. 1 Satz 1 BGB, denn diese Personen sind in Anwendung von Art. 6 Abs. 1 GG bereits keine Dritten (§ 553 Abs. 1 BGB), sondern nahe Familienangehörige. Der Mieter muss die Aufnahme von Familienangehörigen nur anzeigen. Einer Aufnahmeerlaubnis durch den Vermieter bedarf es nicht.

ff) Mitgliedschaften in Parteien und Mietvereinen

Es besteht keine Verpflichtung, über die Zugehörigkeit zu Parteien oder Mietervereinen Auskunft zu geben. Mit den Angaben wird zudem noch keine Aussage zur Bonität des Mietinteressenten bzw. zu dessen Zahlungsfähigkeit und Zahlungswilligkeit getroffen.

gg) Angaben zum Arbeitgeber, zum Beschäftigungsverhältnis und zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine

Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

hh) Einkommensverhältnisse

Die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens wäre jedoch auch die Angabe einer bestimmten Betragsgrenze durch den Mietinteressenten ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird. Im Hinblick auf die monatlichen Belastungen ist die Erfragung der Forderungsgründe (Unterhaltsverpflichtungen, Darlehensverbindlichkeiten etc.) unzulässig, da dies für die Beurteilung der Bonität nicht erforderlich ist.
Fragen nach den Einkommensverhältnissen sind unzulässig, wenn die Mietzahlungen vollständig von dritter Stelle für den Mieter übernommen und direkt an den Vermieter geleistet werden sollen, was bei Empfängern von Arbeitslosengeld II der Fall sein kann. Empfänger von Arbeitslosengeld II müssen für die Durchführung einer solchen Direktzahlung gegenüber dem Jobcenter eine entsprechende Erklärung abgeben, § 22 Abs. 7 Satz 1 SGB II. Direktzahlungen an den Vermieter werden nach § 22 Abs. 7 Satz 2 SGB II von Amts wegen vorgenommen, wenn eine zweckentsprechende Verwendung der gewährten Mittel durch den Empfänger von Arbeitslosengeld II nicht sichergestellt ist.

ii) Angaben zu bisherigen Vermietern

Fragen nach den Kontaktinformationen aktueller oder früherer Vermieter des Mietinteressenten (z. B. Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig. Solche Angaben wären für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich und würden eine dem Grundsatz der Direkterhebung (§ 4 Abs. 2 Satz 1 BDSG) widersprechende Datenerhebung bei Dritten über den Mietinteressenten ermöglichen.

c) Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten

Der künftige Vermieter möchte nun mit dem einzigen Mietinteressenten für eine konkrete Wohnung einen Mietvertrag schließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.

aa) Nachweise zu den Einkommensverhältnissen

Der künftige Vermieter kann bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen darauf hinweisen, dass für den Fall einer positiven Entscheidung für den Mietinteressenten quasi unmittelbar vor Unterzeichnung des Vertrags noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z. B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben. Als Nachweis ist auch eine Bescheinigung des Arbeitgebers ausreichend, dass die Angaben des Mietinteressenten bezüglich der Angabe einer bestimmten Nettobetragsgrenze, die überschritten wird, zutreffend sind.

bb) Vorlage der Selbstauskunft nach Anfrage bei einer Auskunftei

Der künftige Vermieter benötigt Informationen zu den wirtschaftlichen Verhältnissen des Mietinteressenten, um dessen Zahlungsfähigkeit bezüglich des Mietzinses beurteilen zu können. Selbstauskünfte, die Mietinteressenten bei Auskunfteien (z. B. SCHUFA) selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse, als für eine solche Beurteilung erforderlich sind. Schon aus diesem Grund wäre die Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig.

Da die Verwendung von Einwilligungserklärungen gegenüber dem Mietinteressenten in Formularen zur Selbstauskunft nicht als das richtige Mittel zur Datenerhebung anzusehen ist, wäre auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, nicht rechtmäßig. Zur Einholung von Bonitätsauskünften über den Mietinteressenten wäre der Vermieter nur dann befugt, wenn die Voraussetzungen einer gesetzlichen Vorschrift (§ 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG) erfüllt sind.[1)]

[1)] Vgl. zur Einholung von Bonitätsauskünften über Mietinteressenten gegenüber Auskunfteien den Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009 „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig".

Anlage 11

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 19. Februar 2014)

Videoüberwachung in Schwimmbädern Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen.
Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vergleiche OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu

Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur, damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen[1)].

[1)] OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z. B. Beschädigung von Haartrocknern).

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z. B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch – wenn auch nicht ununterbrochen – auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

Anlage 12

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.
Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.
Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.
Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier

beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.
Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Anlage 13

Entschließung
der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2014 in Hamburg

Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden so genannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.
Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.
Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass

die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.
An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.
- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Anlage 14

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfü-

gung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

   Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Anlage 15

Entschließung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 18./19. März 2015 in Wiesbaden

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist[1)]. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

[1)] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Anlage 16

Entschließung
der 90. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 30. September/1. Oktober 2015 in Darmstadt

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können

Anlage 17

Entschließung
der Sondersitzung der Datenschutzbeauftragten
des Bundes und der Länder
am 21. Oktober 2015 in Frankfurt
Positionspapier der DSK

1. Nach dem Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 ist eine Datenübermittlung aufgrund der Safe-Harbor-Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG) nicht zulässig.

2. Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt.

3. Der EuGH stellt fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten ungeachtet von Kommissions-Entscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen.

4. Der EuGH fordert die Kommission und die Datenschutzbehörden auf, das Datenschutzniveau in den USA und anderen Drittstaaten (Rechtslage und Rechtspraxis) zu untersuchen und gibt hierfür einen konkreten Prüfmaßstab mit strengen inhaltlichen Anforderungen vor.

5. Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe-Harbor gestützte Datenübermittlungen in die USA erlangen, werden sie diese untersagen.

6. Die Datenschutzbehörden werden bei Ausübung ihrer Prüfbefugnisse nach Art. 4 der jeweiligen Kommissionsentscheidungen zu den Standardvertragsklauseln vom 27. Dezember 2004 (2004/915/EG) und vom 5. Februar 2010 (2010/87/EU) die vom EuGH formulierten Grundsätze, insbesondere die Randnummern 94 und 95 des Urteils, zugrunde legen.

7. Die Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von

verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen erteilen.

8. Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten. Unternehmen, die Daten in die USA oder andere Drittländer exportieren wollen, sollten sich dabei auch an der Entschließung der DSK vom 27. März 2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und an der Orientierungshilfe „Cloud Computing“ vom 9. Oktober 2014 orientieren.

9. Eine Einwilligung zum Transfer personenbezogener Daten kann unter engen Bedingungen eine tragfähige Grundlage sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.

10. Beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein.

11. Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.

12. Die Kommission wird aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit. Ferner gilt es, zeitnah die Entscheidungen zu den Standardvertragsklauseln an die in dem EuGH-Urteil gemachten Vorgaben anzupassen.
Insoweit begrüßt die DSK die von der Art. 29-Gruppe gesetzte Frist bis zum 31. Januar 2016.

13. Die DSK fordert die Bundesregierung auf, in direkten Verhandlungen mit der US-Regierung ebenfalls auf die Einhaltung eines angemessenen Grundrechtsstandards hinsichtlich Privatsphäre und Datenschutz zu drängen.

14. Die DSK fordert Kommission, Rat und Parlament auf, in den laufenden Trilog-Verhandlungen die strengen Kriterien des EuGH-Urteils in Kapitel V der Datenschutzgrundverordnung umfassend zur Geltung zu bringen.

Anlage 18

Pressemitteilung
vom 31. Januar 2014

Das Auto – Black-Box außer Kontrolle

Gestern hat der Verkehrsgerichtstag 2014 klare Regeln für Autodaten gefordert. Eine Forderung, der sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse ausdrücklich anschließt.

Die moderne technische Automobilausstattung bringt es mit sich, dass – zumindest in neueren Fahrzeugen – umfassende Daten über Fahrverhalten und Fahrroute erhoben werden können. Möglich ist sogar, in Erfahrung zu bringen, wann der Fahrer geschaltet und mit welcher Intensität er wo gebremst hat. Bereits jetzt interessieren sich die Kfz-Versicherer für diese Daten und wollen ihre Versicherten dazu bringen, eine Black-Box einbauen zu lassen, die das Fahrverhalten ebenfalls beobachtet. Es ist auch nicht auszuschließen, dass derjenige, der in einen Unfall verwickelt ist, in gar nicht ferner Zukunft herangezogen werden wird, seine Fahrzeugdaten zu seiner Belastung auslesen zu lassen – ein Verstoß gegen das im Allgemeinen Persönlichkeits-Grundrecht wurzelnde Selbstbelastungsverbot! Als Gegenleistung soll dann zwar die Versicherungsprämie um etwa 5 % gesenkt werden – bei entsprechend negativem Fahrverhalten wird diese jedoch wieder erhöht werden. Ob hierin noch eine freiwillige Datenpreisgabe des Betroffenen gesehen werden kann, wird derzeit kontrovers diskutiert. Die Gefahren einer derartigen Profilbildung sowie das Wecken von Daten-Begehrlichkeiten liegen auf der Hand.

Virulent wird vor diesem Hintergrund auch die Problematik der Überwachung von Beschäftigten, die z. B. den LKW des Arbeitgebers nutzen.

Das Bundesdatenschutzgesetz hinkt der Realität wieder einmal hinterher. Es legt nicht fest, wem die erhobenen Daten gehören und wer sie zu welchen Zwecken verwenden darf. Oftmals wissen die Fahr-

zeugnutzer nicht einmal, welche Daten über sie erhoben werden und wer diese Daten zu welchen Zwecken nutzt.

„Ich werde mich im Rahmen meiner Möglichkeit dafür einsetzen, dass der Bundesgesetzgeber sich der Thematik annimmt, damit für die Autofahrer in Deutschland die Rechtssicherheit wiederhergestellt wird“, so Dr. Lutz Hasse (TLfDI).

Anlage 19

Pressemitteilung
vom 11. Dezember 2014

Weihnachtsgeschenk für den Datenschutz!

Etwas verfrühte Weihnachtsbescherung: Heute hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens über die Auslegung von Art. 3 Abs. 2 der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bestätigt, dass auf eine privat betriebene Videoüberwachungsanlage unter bestimmten Voraussetzungen die Europäische Datenschutzrichtlinie und damit das insoweit gleichlautende Bundesdatenschutzgesetz anwendbar ist.

Bereits in der Presseerklärung vom 23.07.2014 „Videogaga: Europäischer Perspektivenwechsel“ hat der TLfDI auf die Rechtssache C-212/13 beim EuGH und den damit verbundenen Perspektivenwechsel hingewiesen. Gegenstand war eine privat betriebene Videoüberwachungsanlage, die zum Schutz eines Privatgrundstücks auch Teile des öffentlich zugänglichen Raums aufgezeichnet hatte.

Heute hat der EuGH klargestellt: Jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie öffentlich zugänglichen Raum erfasst, fällt in den Anwendungsbereich der Europäische Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes; sie ist damit nur unter den dort geregelten Voraussetzungen zulässig.

Der TLfDI freut sich, dass seine bereits seit mehreren Jahren vertretene Rechtsauffassung durch den EuGH bestätigt wurde. Für Thüringen bedeutet dies, dass der TLfDI weiterhin an seiner Kontrollpraxis festhalten und die Rechtmäßigkeit von privat betriebenen Videoüberwachungsanlagen als zuständige Aufsichtsbehörde prüfen wird. Und: Der TLfDI kann damit BürgerInnen, die von solchen Videoaufnahmen betroffen sind, weiterhin unterstützen – ein guter Tag für den Datenschutz und die Privatsphäre! ☺

Anlage 20

Pressemitteilung
vom 5. Januar 2015

Elektronische Gesundheitskarte ist nun Pflicht!

Seit dem 1. Januar 2015 gilt nunmehr ausschließlich die elektronische Gesundheitskarte (eGK) als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkasse beim Arzt oder Zahnarzt.

Auf der eGK befinden sich alle Daten, die bislang auf der Krankenversichertenkarte enthalten waren sowie zusätzlich das Geschlecht und – außer in den gesetzlich vorgesehenen Ausnahmefällen – ein Lichtbild des Patienten. Hierdurch soll einem Kartenmissbrauch vorgebeugt werden.

Die eGK ist aber darauf ausgerichtet, folgende zusätzliche Funktionen zu erfüllen:

- **Online-Abgleich** der Daten der Karte beim Einlesen in der Praxis mit den bei der Krankenkasse vorliegenden aktuellen Daten des Versicherten; dabei hat die Krankenkasse keinerlei Zugriff auf die beim Arzt vorliegenden Daten;
- Speicherung ärztlicher Verordnungen (sog. **eRezept**) und des Berechtigungsnachweises für EU-Ausländer (sog. **Europäische Krankenversicherungskarte**);
- Zusätzliche Daten können **auf Wunsch des Patienten** gespeichert werden, beispielsweise Notfallversorgungsdaten, ein elektronischer Arztbrief oder persönliche Arzneimittelrisiken und -unverträglichkeiten.

Zunächst soll der Online-Abgleich ab Mitte 2015 in verschiedenen Testregionen erprobt werden, nicht aber in Thüringen. Termine für eine bundesweite Einführung des Online-Abgleichs oder für Tests der weiteren Funktionen stehen noch nicht fest. **Für die Patienten in Thüringen ändert sich also erst einmal nichts.**

Das Projekt wird durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit datenschutzrechtlich begleitet.

Die Kommunikation mit diesen sensiblen Gesundheitsinformationen zwischen Krankenversicherern, Ärzten und Apothekern ist über **ein eigens zu diesem Zweck errichtetes Gesundheitsnetz** vorgesehen, das keine Schnittstelle zum öffentlichen Internet hat. Alle Gesundheitsdaten – auch Rezeptdaten - werden verschlüsselt abgelegt. Sie werden – etwa wenn der Patient dem Arzt oder Apotheker den Zugriff auf diese Daten ermöglichen möchte – durch das gleichzeitige Stecken der eGK und des dem Arzt oder anderen Berechtigten ausgestellten Heilberufsausweises in ein spezielles Kartenlesegerät entschlüsselt.

Darüber hinaus muss der Versicherte einem **Zugriff auf medizinische Daten** durch die Eingabe einer PIN zustimmen. Eine Ausnahme bilden die freiwilligen Notfalldaten, auf die der Heilberufsausweis allein den Zugriff gewährt. Auch für das Entschlüsseln von Rezeptdaten beim Apotheker ist keine PIN erforderlich.

Die Zugriffe auf die eGK werden protokolliert, damit der Versicherte die Zugriffe auf seine Daten einsehen und verfolgen kann.

Mit der vorgesehenen elektronischen Patientenakte wird die eGK voraussichtlich eine weitere Entwicklung erfahren, die der TLfDI beobachten und gegebenenfalls beeinflussen wird.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht für Fragen zur eGK gern zur Verfügung und wird weiter über den Fortgang berichten.

Anlage 21

Pressemitteilung
vom 30. Januar 2015

TLfDI fordert: Deutschland oben ohne – Drohne!

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Da können schon Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, den Nacktbadebereich am See oder in sonstige nicht einfach zugängliche Orte.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) weist darauf hin, dass eine legale Drohnennutzung durch **Private** in Deutschland nur unter äußerst engen Voraussetzungen zulässig ist. Zahlreiche Rechtsvorschriften müssen beachtet werden:

Sobald mit der Kamera Menschen gefilmt und damit personenbezogene Daten erhoben werden, müssen das Recht am eigenen Bild und das Grundrecht auf informationelle Selbstbestimmung beachtet werden. Selbst wenn mögliche datenschutzrechtliche Erlaubnisnormen (§§ 6b, 28 und 32 Bundesdatenschutzgesetz) einschlägig wären, würden in aller Regel die schutzwürdigen Interessen der Betroffenen überwiegen. „**Folglich darf mit der Kamera einer Drohne grundsätzlich niemand gegen seinen Willen gefilmt werden**“, betont der TLfDI.

Leider existieren in Deutschland keine verbindlichen eindeutigen Regelungen speziell für Drohnen im zivilen Bereich. Das will die EU jetzt ändern. Sie fordert strenge Regulierung für zivile Drohnen (http://europa.eu/rapid/press-release_IP-14-384_de.htm). Der TLfDI begrüßt diese Entwicklung ausdrücklich. Da die Drohnennutzung in einigen Bereichen, wie im Straßen- und Eisenbahnbrückenbau oder in der Forst- und Landwirtschaft durchaus sinnvoll sein kann, bedarf es konkreter Bestimmungen, wie der datenschutzgerechte Umgang mit Drohnen auszusehen hat.

Einen guten Überblick über die ***luftverkehrsrechtlichen*** Anforderungen gibt die „Kurzinformation über die Nutzung von unbemannten Luftfahrtsystemen“ (unter http://www.bmvi.de/SharedDocs/DE/Publikationen/LF/unbemannte-luftfahrtsysteme.html?linkToOverview=js).

Anlage 22

Pressemitteilung
Windows 10 – Fenster zur Privatsphäre

Seit ein paar Wochen ist das Produkt Windows 10 von Microsoft auf dem Markt. Microsoft bietet sogar ein kostenloses Upgrade, also den Wechsel von alten Windows Betriebssystemen auf Windows 10 an. Zudem wirbt Microsoft damit, dass Windows 10 „voller fantastischer Innovationen“ steckt. Richtig! Denn Microsoft hat nun für sich entdeckt, dass Daten über die Nutzer und die verwendeten Geräte und deren Standorte innovativ für Microsoft selbst und für seine Geschäftspartner und Tochterunternehmen genutzt werden können.

Welche Gefahren drohen?

Wie durch die Fachpresse mitgeteilt wird, werden nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten an Microsoft übertragen. Außerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich“ angesehen wird (siehe dazu http://www.microsoft.com/de-de/privacystatement/default.aspx, Unterpunkt „Personifizierte Daten, die wir sammeln“ – „Mehr erfahren“ – „Inhalte“)!

Das können Sie tun:

Viele Dienste zur Datensammlung können deaktiviert werden. Dazu müssen Sie bspw. unter dem Punkt „Einstellungen -> Datenschutz“ in den 13 Kategorien Ihre persönlichen Einstellungen vornehmen. Eine ausführliche Anleitung, wie man dies bewerkstelligen kann, ist unter http://www.computerbase.de/2015-07/windows-10-test/7/ zu finden.

!Schützen Sie Ihre Daten und Ihre Privatsphäre!

Anlage 23

Pressemitteilung
vom 6. Oktober 2015

Unsafe harbor – Datenschutzbeauftragter Dr. Hasse: Der EuGH hat den „unsicheren Hafen“ endlich geschlossen

„Mit seinem Urteil zum Safe-Harbor-Abkommen (zu Deutsch: Sicherer-Hafen-Abkommen) hat der Europäische Gerichtshof (EuGH) die Rechtspositionen der Datenschutzbeauftragten des Bundes und der Länder deutlich gestärkt – dies ist ein Meilenstein für den Datenschutz in Europa, Deutschland und in Thüringen“, kommentiert Thüringens Datenschutzbeauftragter, Dr. Lutz Hasse, die Entscheidung der Luxemburger Richter. Der EuGH habe den „unsicheren Hafen“, so Hasse, heute zu Recht geschlossen und dessen Regelungen für ungültig erklärt, weil sie keinen ausreichenden Schutz vor Grundrechtseingriffen durch amerikanische Behörden geboten hätten. „Das haben die deutschen Datenschutzbehörden seit den Enthüllungen Edward Snowdens im Sommer 2013 immer wieder kritisiert“, erinnert Lutz Hasse. Seine KollegInnen und er hatten seit damals die Aussetzung einer Datenübermittlung in die USA, basierend auf dem Safe-Harbor-Abkommen, gefordert, weil dessen Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und der Zweckbindung eines behördlichen Datenzugriffs von US-amerikanischen und anderen Sicherheitsdiensten schlichtweg ignoriert wurden. Erfreut zeigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch über den klaren Hinweis des EuGH, dass die Kommission keine Kompetenz hatte, die Befugnisse der nationalen Datenschutzbehörden mit der Unterzeichnung des Safe-Harbor-Abkommens zu beschränken. Hasse: „Damit stärken die Luxemburger Richter erneut die Unabhängigkeit der Datenschutzbehörden.“ Zudem empfahl Hasse, die geplanten Regelungen der neuen EU-Datenschutz-Grundverordnung im Lichte dieser sehr deutlichen EuGH-Rechtsprechung zu überdenken. „Man muss sich nun die Zeit nehmen, die Auswirkungen dieses wegweisenden Urteils auf die vorgesehene Datenschutz-Grundverordnung zu erkennen und deren Regelungen an der Entscheidung ausrichten“, so der TLfDI.

Anlage 24

"Cyber-Risiken" für Unternehmen – wirtschaftliche Auswirkungen
Veranstaltung der Sektion Nordthüringen
8. Mai 2014

Inhalt:
Artikel 6 Thüringer Verfassung
§ 3 Abs. 1 Thüringer Datenschutzgesetz: Begriffsbestimmungen
§ 4 Abs. 1 Thüringer Datenschutzgesetz: Zulässigkeit der Datenverarbeitung und -nutzung
Checkliste zur Bestellung eines bDSB gemäß § 4 f BDSG
Übersicht Ablauf Bußgeldverfahren
Urteil: United States District Court Az.: 13 Mag. 2814

Anlage 25

Videoüberwachung in Unternehmen: PraxisCampus, Köln
6. Juni 2014

Inhalt:
Einzelfälle aus der Praxis
Gesetzliche Regelung: Was ist zulässig/unzulässig?
Technische und organisatorische Maßnahmen
Eingriffsbefugnisse und Sanktionen

Anlage 26

Datenschutz in der Medizin – UpDate! Leipzig
11. September 2014

Inhalt:
Datenschutz in der Medizin
Datenschutzfallen im medizinischen Bereich
Fallbeispiele

Anlage 27

Workshop Frankfurt am Main „Der Arzt ist weg – wo bleiben die Patientenunterlagen?“ – Rechtsgrundlagen und Umsetzungsfragen zur Aufbewahrung von Patientenakten
2. Oktober 2014

Inhalt:
Fallbeispiele
Praxis-Nachfolger
Kein Nachfolger
Runder Tisch Aktenarchivierung Thüringen
§ 27 b Datenverarbeitung im Auftrag

Anlage 28

Jenaer Datenschutzkolloquium
10. Oktober 2014

Inhalt:
Wer ist der TLfDI?
Wann ist der TLfDI im nicht-öffentlichen Bereich zuständig?
Welche Aufgaben und Befugnisse hat die Aufsichtsbehörde – der TLfDI nach § 38 BDSG?
Exkurs: Kontrollrecht / Berufsgeheimnis
Ordnungswidrigkeiten
Datenschutzrechtliche Grundsätze
Welche Anforderungen stellt das Bundesdatenschutzgesetz (BDSG) an den betrieblichen Datenschutz?
Sonderfälle Videoüberwachung

Anlage 29

HWK Erfurt Veranstaltung
12. November 2014

Datenschutz im Internet

Dipl.–Ing. Jens Keßler

Mitarbeiter Referat 3
Technischer und organisatorischer Datenschutz beim

Thüringer Landesbeauftragten für den Datenschutz und die
Informationsfreiheit (TLfDI)

Inhalt:

Anlage 30

Datenschutz im Schulbereich und Einzelfälle Datenschutz in der Erwachsenenbildung
Landesorganisation der freien Träger in der Erwachsenenbildung e. V. LOFT
21. November 2014

Inhalt:
Der TLfDI!
Was ist Datenschutz?
Datenschutz im Rechtssystem
Welche Regelungen gelten für Bildungseinrichtungen nach BDSG?
Welche Daten darf ich erheben?
Fallstricke bei der Teilnehmerwerbung
Konsequenz bei Verstößen
Regelungen im ThürDSG

Anlage 31

Beschäftigtendatenschutz PraxisCampus, Köln
23. April 2015

Inhalt:
Gesetzliche Regelungen zum Beschäftigtendatenschutz
Videoüberwachung – Was ist zulässig/unzulässig?
Erläuterung anhand von Praxisbeispielen
Technische und organisatorische Maßnahmen
Eingriffsbefugnisse und Sanktionen
Ausblick zum „Beschäftigtendatenschutzgesetz“

Anlage 32

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD)
e.V. Verbandstage 2015
„Moderner Datenschutz: Neue Lösungen – Neue Risiken“
12. Mai 2015

Inhalt:
Aufsichts- oder Ordungswidrigkeitenbehörde?
Wann prüft die Aufsichtsbehörde?
Welche Rechte hat die Aufsichtsbehörde?
Auskunft, § 38 Abs. 3 BDSG
Kontrolle
Anordnung von Maßnahmen
Ordnungswidrigkeiten

Anlage 33

DEHOGA Thüringen Fachgruppensitzung Hotel und Tourismus
20. Mai 2015

Inhalt:
Rechtsgrundlagen
Datenschutzerklärung
Melderecht
Videoüberwachung
Buchung über Dritte

Anlage 34

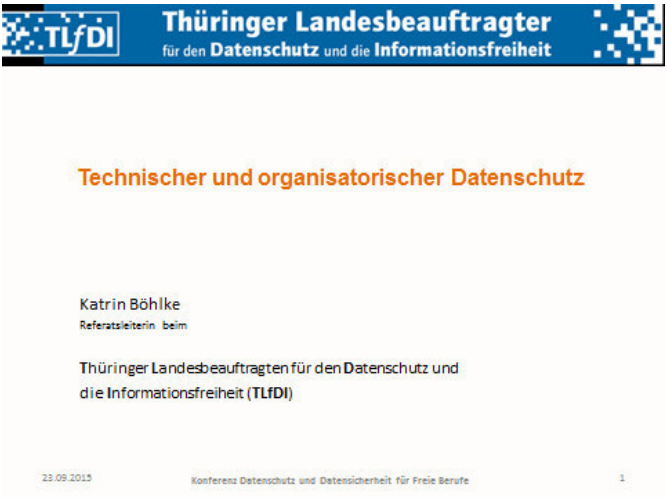
Thüringer Seniorenverband BRH e. V. Artern
10. Juni 2015

Inhalt:
Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?

Anlage 35

Konferenz Datenschutz und Datensicherheit für Freie Berufe (LFB e. V.)
23. September 2015

Inhalt:
Beauftragung externer (IT-)Dienstleister, Auslagerung in die Cloud – wie ist das mit der Verschwiegenheitspflicht von Berufsgeheimnisträgern zu vereinbaren?



Inhalt:
Industrie 4.0 – Was haben die Freien Berufe davon?
De-Mail
Cloud Computing aus technischer Sicht
Sonstiges (nPA, BYOD, .)

Anlage 36

Tagung Autorecht Uni Augsburg
8. Oktober 2015

Inhalt:
Einführung
Entwicklungsstufen und Funktionsweisen
Datenschutzrechtliche Hintergründe
Fahrplan für künftige Entwicklungen

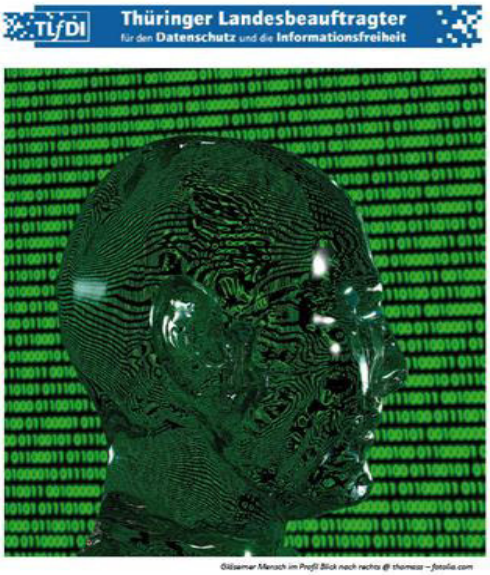
Anlage 37

UpDate! Fachtagung: Datenschutz in der Medizin in Leipzig
12. November 2015

Inhalte:
Europäische Datenschutzgrundverordnung
Safe Harbor Entscheidung des EuGH
OH Aktenarchivierung
E-Health-Apps
Fallbeispiel

Anlage 38

Ausgewählte Veranstaltungen 2014-2015



Alles was zählt -

Algorithmen allmächtig?

am 2. Juli 2014

ab 10:00 Uhr

im Rathaus Erfurt

Inhalt:

„Big-Data-Analysen: Möglichkeiten, Herausforderungen und Gefahren“
Herr Prof. Dr. Kai-Uwe Sattler, TU Ilmenau
"Datenschutz, Humangenetik, Personalisierte Medizin – Ein (zu?) weites Feld"

Herr Prof. Dr. Kay Hamacher, TU Darmstadt

"Amazon weiß, was Sie wollen, bevor Sie das wissen - Wie Statistik und Big Data unsere Freiheit bedrohen (wenn wir nichts dagegen tun)“
Herr Kai Biermann, Redaktion Zeit Online

Medienkunde als eigenes Schulfach - Neuland in Sicht?
10. Februar 2015
im Rathaus Erfurt

Inhalt:

„Datenschutz und Medienbildung“
Herr Edgar Wagner, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

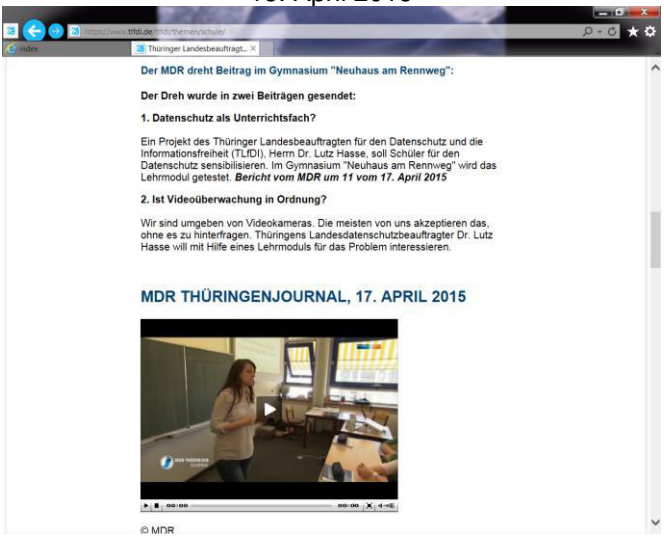
„Medienbildung und Lehrkräfte – Kochen ohne Köche und Rezepte?“
Frau Prof. Dr. Ira Diethelm, Carl von Ossietzky Universität Oldenburg

„Medienkunde und Informatische Bildung -

Pflicht oder Kür?"
Herr Prof. Dr. Steffen Friedrich, Technische Universität Dresden

„Kompetenzen für die digitalisierte (Arbeits-)Welt? Medienkunde, Informatik und ein neuer Begriff von Allgemeinbildung."
Herr Dr. Stephan Pfisterer, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. – BITKOM –
Nachzulesen im Reader zur Tagung.

Veranstaltung zum „Lehrmodul Medienkompetenz"
im Staatlichen Gymnasium Neuhaus/Rwg.
15. April 2015



Ein Projekt des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Lutz Hasse, soll Schüler für den Datenschutz sensibilisieren. Im Gymnasium "Neuhaus am Rennweg" wird das Lehrmodul getestet.

DEN KURZFILM ZUR VIDEOPROBLEMATIK ALS MODUL FÜR DEN SCHULUNTERRICHT

Alltägliche Erfahrung auf Spielplätzen, Sportanlagen und in Geschäften: Kameras, Kameras, Kameras … Erfreulich, wenn sich auch Jugendliche fragen – Was soll das denn? Geht das überhaupt in Ordnung? Diese Thematik greift ein Video auf, das vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) konzipiert und von Studenten der TU Ilmenau hergestellt wurde. Gedacht ist es für den Einsatz an den Thüringer Schulen. Dort ist das Thema Datenschutz auch Gegenstand des Kurses Medienkunde in den Klassenstufen 5 bis 10. Der TLfDI verfolgt das Ziel, dass Datenschutz auch wirklichkeitsnah vermittelt werden kann. So hat seine Behörde ein Unterrichtsmodul für den Einsatz im Unterricht entwickelt, zu dem auch besagter Kurzfilm gehört. Nach Unterrichtserprobung wird das gesamte Modul, bestehend aus Video, Lehrerhandreichung und weiteren Materialien auf der Internetseite des TLfDI und im Thüringer Schulportal downloadfähig sein. Bis dahin können Neugierige ja schon mal einen Blick in das Video werfen. © TLfDI
Mehr Infos finden Sie unter https://www.tlfdi.de/tlfdi/themen/schule/

Abkürzungsverzeichnis

Abkürzung	Bedeutung
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabeordnung
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
BAG	Berufsausübungsgemeinschaft
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BVerfGE	Bundesverfassungsgerichtsentscheidung
bzw.	beziehungsweise
ChemVerbotsV	Chemikalien-Verbotsverordnung
DSB	Beauftragter für den Datenschutz
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche in Deutschland
EDV	Elektronische Datenverarbeitung
EEG	Erneuerbare-Energien-Gesetz
eIDAS	electronic identification and trust services
EnWG	Energiewirtschaftsgesetz
EuGH	Europäischer Gerichtshof
evtl.	eventuell

GBO	Grundbuchordnung
gem.	gemäß
GFAW	Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH
GG	Grundgesetz
ggf.	gegebenenfalls
GPS	Global Positioning System
GWG	Geldwäschegesetz
HGB	Handelsgesetzbuch
HGB	Handelsgesetzbuch
Hs.	Halbsatz
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
IFS	International Featured Standards
IHK-Ost	Industrie- und Handelskammer Ostthüringen
IMB	inoffizieller Mitarbeiter
JuSchG	Jugendschutzgesetz
KRITIS-Strategie	Strategie zum Schutz Kritischer Infrastrukturen
KunstUrhG	Kunsturhebergesetz
LKA	Landeskriminalamt
LNVG	Lokale Nahverkehrsgesellschaft
MBO	Muster-Berufsordnung
MfS	Ministerium für Staatssicherheit
MiLoG	Mindestlohngesetz
MVZ	Medizinisches Versorgungszentrum
Nr.	Nummer
o. g.	oben genannte
OH	Orientierungshilfe
OH A	Orientierungshilfe Aktenaufbewahrung
ÖPNV	Öffentlicher Personennahverkehr

PAuswG	Personalausweisgesetz
PostG	Postgesetz
Rn.	Randnummer
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
sog.	so genannte
SPNV	Schienengebundener Personennahverkehr
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Stasi-Unterlagen-Gesetz
TB	Tätigkeitsbericht
ThürBestG	Thüringer Bestattungsgesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürKHG	Thüringer Krankenhausgesetz
ThürSchulG	Thüringer Schulgesetz
ThürSchulO	Thüringer Schulordnung
ThürVermGeoG	Thüringer Vermessungs- und Geoinformationsgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLVermGeo	Thüringer Landesamt für Geoinformation und Vermessung
TLVwA	Thüringer Landesverwaltungsamt
TMASGFF	Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie
TOMs	technische-organisatorische Maßnahmen
u. a.	unter anderem
UAG	Unterarbeitsgruppe
ÜBAG	überörtliche Berufsausübungsgemeinschaft
UStG	Umsatzsteuergesetz
usw.	und so weiter

UVV	Unfallverhütungsvorschriften
VDV	Verband Deutscher Verkehrsunternehmen
WEG	Wohnungseigentumsgemeinschaft
WoEigG	Wohnungseigentumsgesetz
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Sachregister