

U n t e r r i c h t u n g

durch die Präsidentin des Landtags

Neunter Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz hat den oben genannten Bericht mit folgendem Schreiben vom 8. Juni 2012 zugeleitet:

"Anliegend sende ich Ihnen den 9. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz mit der Bitte um Kenntnisnahme und zur weiteren Veranlassung."

Birgit Diezel
Präsidentin des Landtags

Hinweis der Landtagsverwaltung:

Der Tätigkeitsbericht wurde an die Mitglieder des Landtags am 8. Juni 2012 als Broschüre verteilt. Er kann auch im Abgeordneteninformationssystem und im Internet unter www.parldok.thueringen.de/parldok unter der o. a. Drucksachennummer eingesehen werden.

Gemäß § 52 Abs. 5 GO wurde der Bericht sowie die gemäß § 40 Abs. 1 Satz 3 des Thüringer Datenschutzgesetzes zu erwartende Stellungnahme der Landesregierung zum Bericht an den Innenausschuss überwiesen.

9. Tätigkeitsbericht

des Thüringer Landesbeauftragten für den Datenschutz

Berichtszeitraum: 1. Januar 2010 bis 31. Dezember 2011
Zitervorschlag: 9. TB LfD Thüringen

Der 9. Tätigkeitsbericht steht im Internet unter der
Adresse
www.thueringen.de/datenschutz zum Abruf bereit.

Erfurt, im Juni 2012

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

Vorbemerkung	8
1 Schwerpunkte im Berichtszeitraum	8
2 Allgemeine Entwicklungen im Datenschutz 11	
2.1 Entwicklungen auf Bundesebene	11
2.2 Online-Petitionen im Landtag?	13
2.3 Novellierung des ThürDSG.....	13
2.4 Zensus 2011	14
3 Europäischer und Internationaler Datenschutz	19
3.1 Gesamtkonzept für den Datenschutz in der Europäischen Union	19
3.2 Keine Vorratsdatenspeicherung und Rasterung von Flugpassagierdaten!.....	20
3.3 Defizite bei der Umsetzung des SWIFT-Abkommens...	21
4 Neue Medien – Rundfunk – Telekommunikation	23
4.1 Einsatz von Webanalyseprogrammen auf Behördenseiten	23
4.2 IPv6: Datenschutz ins Netz einbauen!.....	24
4.3 Chance zum datensparsamen Rundfunkgebühren- einzug verpasst	26
4.4 Notrufortung von Mobilfunkteilnehmern durch Rettungsleitstellen	28
5 Kommunales	31
5.1 Ergebnisse der Kommunalkontrollen	31
5.2 Veröffentlichungen im Internet durch Kommunen	32
5.3 Verstöße gegen das Postgeheimnis	35
5.4 Mietwerterhebung unter Mitwirkung privater Dritter oder aus eigener Kraft	37

5.5	Datenschutzrechtliche Kontrolle von Frei- und Hallenbädern	39
5.6	Löschfristen.....	42
5.7	Zeiterfassung im Kindergarten.....	44
5.8	Firmenumsatz und Fremdenverkehrsabgabe - Fortsetzung.....	46
5.9	Bundesmeldegesetz/Fortentwicklung des Meldewesens	47
5.10	Zweckentfremdung der Hotelmeldedaten	48
5.11	Zugriffsprotokollierung und Auswertung im Meldeamt	50
5.12	Zentrales Personenstandsregister	52
5.13	Nutzung von Sterbebüchern in Archiven	54
5.14	Hundehalterregister mit Mängeln.....	55
6	Personaldaten	59
6.1	Beschäftigtendatenschutz immer noch nicht geregelt	59
6.2	Umgang mit amtsärztlichen Gutachten	60
6.3	Umgang mit Personalunterlagen zur Stasiüberprüfung in der Thüringer Polizei.....	62
6.4	Videüberwachung in den Pausenräumen der Uniklinik Jena	64
7	Polizei.....	66
7.1	Körperscanner nur mit Datenschutz	66
7.2	Datenverarbeitungen beim Papstbesuch.....	67
7.3	Unzulässige Zuverlässigkeitsprüfung auch noch mit veralteten Daten	68
7.4	Kein Datenabgleich zur Verdachtsgewinnung	70
7.5	Neugier von Kollegen	72
7.6	Erweitertes Verfahren in der Zentralen Bußgeldstelle geprüft	74
7.7	Aktenzeichen darf nicht ins Adressfeld.....	75
8	Verfassungsschutz	78
8.1	Evaluierung und Verlängerung der Terrorismusbekämpfungsgesetze	78
8.2	NADIS neu – Probleme mit der Volltextsuche	80
8.3	Hosting der Amtsdatei des TLFV durch das BfV nur mit ausreichender Kontrolle	82

9	Finanzwesen	85
9.1	Haushaltsmanagementsystem (HAMASYS).....	85
9.2	Was darf das Finanzamt bei der Sachverhalts- ermittlung?	87
9.3	Automatische Anzeige des Kontostands nach Verfügungen am Geldautomaten	88
10	Justiz	90
10.1	Vorratsdatenspeicherung – quo vadis?.....	90
10.2	Keine Quellen-TKÜ ohne gesetzliche Grundlage in der Strafprozessordnung	90
10.3	Einschränkung der Funkzellenabfrage	93
10.4	Datenschutzaspekte bei der Überwachung von entlassenen Intensivtätern	95
11	Gesundheits- und Sozialdatenschutz	98
11.1	Krankenhausinformationssystem – eine Orientierungshilfe und deren Umsetzung.....	98
11.2	Errichtung von Pflegestützpunkten	100
11.3	Sozialamt muss Daten beim Betroffenen erheben.....	101
11.4	Rote Windelsäcke für Inkontinente	102
11.5	Vertretung des Amtsarztes durch Private	103
11.6	Datensparsame Umsetzung des Bildungspaketes?	104
11.7	Zuständigkeitswechsel bei den Jobcentern.....	106
11.8	Datenhungrige ARGE	106
11.9	Mindestanforderungen bei Anbindung an medizinische Netze	108
12	Wirtschaft, Arbeit, Bau und Verkehr	109
12.1	Solarkataster zur Solarpotentialanalyse.....	109
12.2	Intelligente Stromzähler – neueste Entwicklungen	110
12.3	Stadtwerke Erfurt verlangten unnötige Daten als Nachweis	111
12.4	Weitergabe von Daten aus dem Gewereregister.....	112
12.5	Neues Einlasssystem an der Ski-Arena Silbersattel	113
12.6	Kfz-Halterauskunft über Umwege nicht zulässig.....	115
12.7	Verkehrszählung per Video in Bad Lobenstein.....	116

13	Bildung, Wissenschaft, Forschung	118
13.1	Erhebungsbogen zur Vorschuluntersuchung.....	118
13.2	Braucht jede Schule einen Datenschutzbeauftragten?..	119
13.3	Datensparsamkeit bei Berufswahlveranstaltungen mit Schülern	120
13.4	Verkehrssicherheitsforschungsvorhaben RETISS.....	121
13.5	Sicherheitsforschung muss Folgen für Persönlichkeitsrechte im Blick behalten	123
14	Entwicklungen der automatisierten Daten- verarbeitung	125
14.1	Cloud-Computing.....	125
14.2	RFID-Selbstregulierung funktioniert nicht.....	127
14.3	Sicheres Löschen von Festplatten	128
14.4	Cookies und Co	131
15	Technische Entwicklungen in der Thüringer Landesverwaltung	135
15.1	Kontrollen der DMS in den obersten Landesbehörden	135

Anlagen

Entschliefungen der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart

Anlage 1	Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!	137
Anlage 2	Ein modernes Datenschutzrecht für das 21. Jahrhundert.....	139
Anlage 3	Keine Vorratsdatenspeicherung!	142
Anlage 4	Körperscanner - viele offene Fragen.....	143
Anlage 5	Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich	145
Anlage 6	Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Kranken- versicherung	147

Entschlieungen zwischen den Konferenzen 2010

Anlage 7	Rundfunkfinanzierung: Systemwechsel nutzen fur mehr statt weniger Datenschutz	149
Anlage 8	Erweiterung der Steuerdatenbank enthalt groe Risiken	151
Anlage 9	Beschaftigtendatenschutz starken statt abbauen.....	153

Entschlieungen der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Lander am 3./4. November 2010 in Freiburg

Anlage 10	Keine Volltextsuche in Dateien der Sicherheitsbehorden	156
Anlage 11	Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs	158
Anlage 12	Forderung des Datenschutzes durch Bundesstiftung....	161

Entschlieungen der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Lander am 16./17. Marz 2011 in Wurzburg

Anlage 13	Beschaftigtendatenschutz starken statt abbauen.....	162
Anlage 14	Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV- Systemen an medizinische Netze	165
Anlage 15	Ohne gesetzliche Grundlage keine Tele- kommunikationsuberwachung auf Endgeraten	167
Anlage 16	Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!.....	169
Anlage 17	Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens - dringender Handlungs- bedarf auf nationaler und europaischer Ebene	171
Anlage 18	Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen.....	173

Entschlieungen zwischen den Konferenzen 2011

Anlage 19	Funkzellenabfrage muss eingeschrankt werden!.....	175
-----------	--	-----

**EntschlieÙungen der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Lander am 28./29. September 2011 in
Munchen**

Anlage 20	Datenschutz bei sozialen Netzwerken jetzt verwirklichen!	177
Anlage 21	Datenschutz als Bildungsaufgabe.....	179
Anlage 22	Anonymes elektronisches Bezahlen muss moglich bleiben!.....	182
Anlage 23	Antiterrorgesetze zehn Jahre nach 9/11 – Uberwachung ohne Uberblick.....	184
Anlage 24	Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing.....	186
Anlage 25	Einfuhrung von IPv6 steht bevor: Datenschutz ins Netz einbauen!	188
Anlage 26	Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!	191

Vorbemerkung

Der vorliegende 9. Tätigkeitsbericht ist in seiner ursprünglichen Fassung vom Amtsvorgänger gefertigt worden. Da der 9. Tätigkeitsbericht jedoch vom derzeitigen Amtsinhaber dem Landtag und der Landesregierung zu erstatten und zu verantworten ist, wurden im zwischenzeitlich für erforderlich erachteten Umfang Änderungen nicht Sinn entstellender Art vorgenommen, die vereinzelt auch der Erwärmung des datenschutzrechtlichen Klimas dienen sollen.

1 Schwerpunkte im Berichtszeitraum

Der TLfD hat im vergangenen Berichtszeitraum wieder zwei repräsentative Vor-Ort-Kontrollen durchgeführt. So wurde auf der Grundlage einer landesweiten Umfrage in insgesamt elf Schwimmbädern der Einsatz von Videoüberwachungstechnik kontrolliert (5.5). Dabei mussten in zehn Fällen zum Teil erhebliche Verstöße gegen den Datenschutz festgestellt werden. Dies betraf im gravierendsten Fall die Anfertigung von Videoaufnahmen in der Sauna bis hin zu kleineren Verstößen wie die fehlenden Hinweise auf die Kameras. Die Kontrollen sind bislang noch nicht abgeschlossen. Derzeit wird mit den Betreibern nach Lösungen gesucht, wie die festgestellten Mängel beseitigt werden können. Allerdings musste bereits in zwei Fällen eine formelle Beanstandung nach § 39 ThürDSG ausgesprochen werden, weil man sich in Mühlhausen und Ichtershausen geweigert hatte, die geforderten Maßnahmen umzusetzen. Hier werden mithilfe der zuständigen Rechtsaufsichtsbehörden die Datenschutzrechte durchzusetzen sein. Ein Teil der Schwimmbadbetreiber hat die Forderungen des TLfD erfüllt, mit den übrigen sind noch Gespräche zu führen. Die andere Querschnittskontrolle betrifft den datenschutzgerechten Umgang mit Patientendaten in Krankenhausinformationssystemen (11.1). Hierzu hat die Datenschutzkonferenz eine Orientierungshilfe herausgegeben, deren Umsetzung in sechs Krankenhäusern kontrolliert worden ist. Auch diese Kontrollen sind noch nicht abgeschlossen. Das Grundproblem liegt darin, dass es sich dabei um sensible Daten handelt, auf die nicht mehr Personen im Krankenhaus Zugriff haben sollen, als unbedingt erforderlich ist. Andererseits beanspruchen Ärzte und Pflegekräfte die bestmögliche

Information über den Patienten, um diesen optimal behandeln zu können. Diese beiden Positionen sind gegeneinander abzuwägen. Einfluss auf diese Diskussion haben zudem die auf dem Markt befindlichen Patienteninformationssysteme, da manche Datenschutzeinstellung in dem jeweiligen Krankenhaus gar nicht vorgenommen werden kann, sondern durch die Hersteller bereits in die Software eingearbeitet werden muss. Die bisherige Behandlung der festgestellten Probleme ist von allen Seiten von dem Bemühen getragen, zu tragfähigen Lösungen zu kommen. Deshalb war bislang keine formelle Beanstandung auszusprechen.

Die Abarbeitung der repräsentativen Kontrolle der Kommunen aus den Jahren 2008 und 2009 hat im letzten Berichtszeitraum nochmals enorme Kapazitäten gebunden und gestaltete sich teilweise sehr mühsam. Wegen mangelhafter bzw. zögerlicher Beseitigung der Defizite mussten daher nochmals fünf Kommunen beanstandet werden (5.1). Nicht nur die untere Verwaltungsebene, sondern auch zwei Ministerien bedurften im Berichtszeitraum einer formellen Beanstandung. Das betraf zum einen das TFM (9.1), das sich zunächst weigerte, das Haushaltsmanagementsystem (HAMASYS) so zu gestalten, dass nicht landesweit in allen Behörden für fast 4000 Mitarbeiter über 200.000 Datensätze zu Bankverbindungsdaten der Zahlungspartner im Zugriff stehen, obwohl es dafür keine Rechtsgrundlage gibt. Die zweite Beanstandung an die Adresse eines Ministeriums war an das TJM (10.2) gerichtet, das sich sträubte, dem TLfD Unterlagen der Staatsanwaltschaft zu einem laufenden Strafverfahren vorzulegen, bei dem eine Quellen-TKÜ angeordnet worden war und das TJM die Kontrollkompetenz des TLfD bestritten hat. Von den im Berichtszeitraum insgesamt elf ausgesprochenen Beanstandungen betraf eine weitere die unzulässige Forderung der Verwaltungsgemeinschaft Rennsteig an einen Unternehmer zur Angabe seines Jahresumsatzes zur Berechnung der Fremdenverkehrsabgabe (5.8). Schließlich musste die Polizeidirektion Nordhausen (7.3) wegen einer unzulässigen Zuverlässigkeitsprüfung beanstandet werden.

Große Bedeutung für die Datenschutzentwicklung hatte im Berichtszeitraum die Novellierung des ThürDSG (2.3). Die vom Europäischen Gerichtshof in seinem Urteil vom 9. März 2010 geforderte völlige Unabhängigkeit des TLfD ist mit der Übertragung der Auf-

gaben der Aufsichtsbehörde für den nicht-öffentlichen Bereich vom Landesverwaltungsamt auf den TLfD personell bisher nicht umgesetzt worden. Die Gefährdungen des Grundrechts der informationellen Selbstbestimmung gerade auch im nicht-öffentlichen Bereich sind unbestritten. Mit diesem gesetzlich beträchtlich erweiterten Aufgabenspektrum sollte eine Aufstockung des Personals in Referatsstärke (mind. 5 Stellen) einhergehen. Diese Logik hat in der personellen Ausstattung der Datenschutzbeauftragten der anderen Bundesländer denn auch ihren deutlichen Niederschlag gefunden; der TLT möge daher ebenso verfahren.

Aufgrund von Beschwerden der Bürger hat der TLfD in den vergangenen Jahren wiederum eine Vielzahl von Hinweisen auf datenschutzrechtliche Mängel erhalten, denen in jedem Einzelfall nachgegangen wurde. So führte ein Hinweis dazu, die Videoüberwachung in den Schwimmbädern einer genaueren Prüfung zu unterziehen (5.5). Eine Vielzahl von Beschwerden machte Defizite in der Datenverarbeitung durch die Polizei deutlich (7.3; 7.4; 7.5 und 7.7), die zum Teil förmlich beanstandet werden mussten oder aber noch nicht abgestellt sind.

Weiterhin zunehmend sind die Beratungen der öffentlichen Stellen und des Gesetzgebers in datenschutzrechtlichen Fragen (z. B. 2.2, 2.3, 2.4, 4.4, 5.2, 5.12, 5.14, 12.1, 13.4, 13.5); eine entsprechend zunehmende Akzeptanz des erteilten fachlichen Rates wäre wünschenswert.

Die stetig steigenden Aufgaben des TLfD können mit den bisherigen Ressourcen nur noch sehr eingeschränkt bewältigt werden. Entsprechende signifikante Abhilfe tut kurzfristig Not, um den Schutz der Bürger gewährleisten zu können.

2 Allgemeine Entwicklungen im Datenschutz

2.1 Entwicklungen auf Bundesebene

Eine grundlegende Modernisierung des Datenschutzrechts unter den Bedingungen des 21. Jahrhunderts wird von den Datenschutzbeauftragten schon seit Jahren gefordert. Unter Vorsitz des BfDI hat eine Arbeitsgruppe der Datenschutzbeauftragten ein Eckpunktepapier mit dem Titel „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ erarbeitet und dessen Kernthesen in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Anlage 2) veröffentlicht. Das Papier ist unter www.thueringen.de/datenschutz unter der Rubrik Veröffentlichungen im Untermenü Grundsatzpapiere zugänglich. Mit diesem Papier soll die Diskussion im Bund, aber auch in den Ländern sowie auf europäischer Ebene zur Modernisierung des Datenschutzrechts vorangetrieben werden. Unter dem Titel „Moderner Datenschutz im 21. Jahrhundert“ veranstalteten die Datenschutzbeauftragten des Bundes und der Länder am 4. Oktober 2010 im Berliner Abgeordnetenhaus dazu ein Symposium mit Experten aus Politik, Wissenschaft, Wirtschaft und Verwaltung. Staatssekretärin Cornelia Rogall-Grothe vom Bundesinnenministerium legte den Schwerpunkt ihres Vortrages auf die geplanten gesetzgeberischen Maßnahmen. Dazu gehört die Regulierung der Profilbildung, die nicht pauschal verboten, sondern mit der Einwilligung des Betroffenen auch zugelassen werden soll. Außerdem soll die Zweckbindung der Daten verbessert und die Transparenz der Datenverarbeitung erhöht werden sowie die Ausübung der Betroffenenrechte auch per Mausklick möglich sein. Anzustreben sei z. B. auch das Vergessen der Daten im Internet durch Verfallsdatum und Einsatz eines digitalen Radiergummis, die datenschutzgerechte Gestaltung von Verfahren (privacy by design) und die Verpflichtung zu datenschutzrechtlichen Grundeinstellungen (privacy by default) z. B. bei der Nutzung von sozialen Netzwerken. Prof. Dr. Friedemann Mattern von der Technischen Hochschule Zürich entwickelte z. T. sehr provokante Szenarien, welche Folgen die Verarbeitung personenbezogener Daten in einer Welt von smarten Objekten, smarter Energie und smarter Daten haben könnte. Die anschließende Podiumsdiskussion bestätigte den dringenden Handlungsbedarf zur Schaffung angemessener Regelungen vor allem für die Verarbeitung von Daten im Internet und in mobil vernetzten IT-Systemen. Aller-

dings muss in der weiteren Diskussion auch beachtet werden, dass v. a. die jüngere Generation sehr viele Daten über sich selbst ganz bewusst preisgibt. Bislang wurden die Vorschläge kaum in konkrete Gesetzesfassungen aufgenommen. Auf Bundesebene sind trotz der Ankündigung im Koalitionsvertrag bislang keine konkreten Gesetzgebungsmaßnahmen zur Modernisierung des BDSG erkennbar. So wie es scheint, soll dies wieder einmal auf die lange Bank geschoben werden. Den Vorwand bietet diesmal die Ankündigung der EU-Kommission, ein Gesamtkonzept für den Datenschutz in der Europäischen Union vorzulegen (s. u. 3.1).

Vorschläge zur Anpassung des Datenschutzrechts an die aktuellen technischen Bedingungen liegen vor; diese sollten zügig umgesetzt werden.

Der Datenschutz soll nach dem Koalitionsvertrag durch die Einrichtung einer Stiftung gestärkt werden. Im Berichtszeitraum haben sich die Aktivitäten verstärkt, eine solche Stiftung Datenschutz einzurichten. Als eine von deren Aufgaben kommt die Prüfung von Produkten und Dienstleistungen auf ihre Datenschutzfreundlichkeit in Betracht. Außerdem kann sie Bildung im Bereich des Datenschutzes stärken und den Selbstdatenschutz unterstützen. Problematisch kann eine Stiftung aus Sicht der Datenschutzbeauftragten dann werden, wenn deren Aufgaben nicht klar von den Aufsichts- und Kontrollaufgaben der Aufsichtsbehörden abgegrenzt sind. So darf sich die Stiftung nicht in Widerspruch zur Kontrolltätigkeit der Datenschutzbehörden setzen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer EntschlieÙung (Anlage 12) darauf hingewiesen, dass eine solche Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperieren sollte. Obwohl es zunächst geplant war, hat die Stiftung im Jahr 2011 ihre Arbeit noch nicht aufgenommen.

Eine Stiftung Datenschutz kann in Teilbereichen die Arbeit der Datenschutzbeauftragten ergänzen. Allerdings darf sie nicht in die Kernkompetenzen der Datenschutzkontrollbehörden eingreifen, da ansonsten der Datenschutz eher geschwächt als gestärkt würde.

2.2 Online-Petitionen im Landtag?

Wie bereits im letzten Tätigkeitsbericht (8. TB, 2.) erwähnt, ist ein Gesetzentwurf der Fraktion DIE LINKE zur Ermöglichung von Online-Petitionen in der letzten Legislaturperiode nicht mehr beschlossen worden und daher der Diskontinuität anheimgefallen. In der laufenden Legislaturperiode hat die Fraktion DIE LINKE einen neuen Versuch gestartet und einen im Wesentlichen gleichen Entwurf eines Gesetzes zur Änderung des Thüringer Gesetzes über das Petitionswesen und weiterer kommunalrechtlicher Regelungen (LT-Drs. 5/2673) vorgelegt. Allerdings waren in diesem Entwurf bereits die in der Anhörung zum Vorentwurf gemachten Änderungsvorschläge weitgehend aufgegriffen worden. Das betraf auch die Vorschläge des TLfD. So konnte sich der TLfD bei einer erneut durchgeführten mündlichen Anhörung zu dem Gesetzentwurf darauf beschränken, zum Schutz vor einer Petitionseinlegung unter falscher Identität auf die Möglichkeiten des elektronischen Identitätsnachweises für Inhaber des neuen elektronischen Personalausweises hinzuweisen. Diese Funktion könnte auch im elektronischen Petitionsverfahren dafür genutzt werden, um sich von der Identität des Urhebers Gewissheit zu verschaffen. Da nicht alle Bürger diese Möglichkeiten nutzen oder noch nicht über einen solchen neuen Personalausweis verfügen, könnte diese Möglichkeit als Option in § 4 Petitionsgesetz (Form der Petition) aufgenommen werden.

Ob im TLT künftig Online-Petitionen möglich sein werden, war bei Redaktionsschluss noch nicht absehbar, da das Gesetzgebungsverfahren noch nicht abgeschlossen ist.

2.3 Novellierung des ThürDSG

Über die Notwendigkeit einer Modernisierung des ThürDSG wurde bereits berichtet; ebenso über das Urteil des Europäischen Gerichtshofs vom 9. März 2010 (Az.: C-518/07), das die Länder verpflichtet, die Datenschutzaufsichtsbehörden mit völliger Unabhängigkeit auszustatten (vgl. 8. TB, 2.). Beides hat die Landesregierung in einem Entwurf eines Gesetzes zur Änderung des Thüringer Datenschutzgesetzes und anderer Vorschriften aufgegriffen. Allerdings sind aus Sicht des TLfD nicht alle Probleme angegangen worden. So blieben die stark zunehmenden Datenverarbeitungen über funkver-

netzte Dienste wie z. B. RFID oder Fernmess- und Fernwirkdienste etwa beim Einsatz sogenannter Smart Meter unberücksichtigt. Da solche Technologien auch von öffentlichen Unternehmen (z. B. Zweckverbänden) eingesetzt werden können, hatte der TLfD eine Regelung der dabei zu beachtenden besonderen Transparenz- und Einwilligungserfordernisse vorgeschlagen. Unberücksichtigt blieb zudem, die bei öffentlichen Stellen (v. a. den Kommunen) bestehende große Rechtsunsicherheit zu beseitigen, unter welchen Voraussetzungen persönliche Daten von Bürgern, Mandatsträgern und Behördenmitarbeitern im Internet veröffentlicht werden dürfen. Da eine vorgeschlagene Regelung im ThürDSG und in der ThürKO nicht erlassen wurde, ist eine Internetveröffentlichung im kommunalen Bereich nach wie vor nur sehr eingeschränkt zulässig (s. u. 5.2). Schließlich sind auch die Vorschläge des TLfD zur Schaffung wirksamer Eingriffsbefugnisse des Datenschutzbeauftragten und zur Informationspflicht der Datenverarbeiter bei Datenpannen gegenüber den Betroffenen und dem Landesbeauftragten nicht aufgegriffen worden. Damit hätten die Rechte der Betroffenen gestärkt und die Einhaltung der Datenschutzvorschriften verbessert werden können. Die vollständigen Änderungsvorschläge des TLfD zum ThürDSG sind auf der Homepage des TLfD unter der Rubrik Veröffentlichungen im Untermenü Grundsatzpapiere abrufbar.

Mit der Novelle des ThürDSG im Jahr 2011 wurde ein Teil des dringenden Änderungs- und Ergänzungsbedarfs im Datenschutzrecht abgearbeitet. Es dürfen nicht wieder zehn Jahre vergehen, bis die notwendigen weiteren Modernisierungsschritte gegangen werden. Der TLfD wird zu gegebener Zeit Vorschläge unterbreiten.

2.4 Zensus 2011

Mit Stichtag 9. Mai 2011 wurde im wiedervereinigten Deutschland erstmals eine Volkszählung (sogenannter Zensus) durchgeführt, bei der auch Verwaltungsregister, z. B. der Meldeämter und der Bundesagentur für Arbeit, genutzt wurden. Die Pflicht der Beteiligung Thüringens an dem Zensus 2011 ergibt sich aus der EU-Verordnung über Volks- und Wohnungszählungen vom 9. Juli 2008 sowie aus dem Bundesgesetz zum Zensus 2011. Im Juni 2010 hat der TLT das Ausführungsgesetz zum Zensusgesetz 2011 verabschiedet, das die organisatorische Durchführung der Zählung durch die Kommunen

und das TLS regelt sowie wichtige Vorkehrungen zur Sicherung des Statistikgeheimnisses sowie zur Trennung der Statistik vom Verwaltungsvollzug enthält. Hierzu hatte der TLfD bereits bei der Erarbeitung des Gesetzentwurfs durch die Thüringer Landesregierung Ergänzungshinweise gegeben, die in Gänze in den Entwurf eingearbeitet wurden.

Nach den Vorschriften des Zensusgesetzes 2011 nehmen die informationstechnischen Aufgaben die statistischen Ämter der Länder von Nordrhein-Westfalen, Sachsen und Bayern arbeitsteilig wahr, wobei diese auch datenschutzrechtliche Verantwortung für die zentral gespeicherten Daten tragen. Daher galt es für die Datenschutzbeauftragten des Bundes und der Länder, vor Beginn der Arbeiten zum Zensus Konsens darüber herzustellen, dass auch die datenschutzrechtliche Kontrolle der Datenverarbeitungen in den „beauftragten“ Statistischen Ämtern nur diesen Landesbeauftragten für den Datenschutz obliegen. Dies war vorab zur Klärung der datenschutzrechtlichen Zuständigkeit bei der Bearbeitung von eventuellen Eingaben von Bedeutung und hat zur Folge, dass z. B. die Kontrolle der Verarbeitung nach § 6 Zensusgesetz (ZensG) 2011 (Gebäude- und Wohnungszählung), soweit sie im Statistischen Landesamt des Freistaats Sachsen erfolgt, ausschließlich dem Sächsischen Datenschutzbeauftragten obliegt.

Das TLS hatte ursprünglich zur Durchführung des Zensus 2011 geplant, die Arbeiten „Druck und Versand der Erhebungsunterlagen“ sowie „Beleglesen der ausgefüllten Erhebungsbögen“ im Rahmen einer Datenverarbeitung im Auftrag von Privatunternehmen durchführen zu lassen. Der TLfD hat gegenüber dem TLS die Auffassung vertreten, dass die geplante Vergabe von Arbeiten zum Druck und Versand sowie zur Beleglesung auf der Grundlage des § 7 ThürStatG (Vergabe statistischer Arbeiten) grundsätzlich erfolgen könne, da dem Thüringer Landesgesetzgeber die Gesetzgebungskompetenz auch bei der Durchführung von Bundesstatistiken für das Verwaltungsverfahren zusteht. Er hat allerdings zu bedenken gegeben, dass es einen Unterschied hinsichtlich der Sensibilität der zu verarbeitenden Daten zwischen den Leistungen zum Druck- und Versand einerseits sowie zur Beleglesung und Erfassung der Daten andererseits gebe. So dürfte es sich bei den für den Druck und Versand verwendeten Adressdaten um Daten geringerer Sensibilität als bei

den ausgefüllten Einzelbögen handeln. Zudem war beim Druck und Versand eine verschlüsselte Verarbeitung bis zum Druck der Adressen vorgesehen, was eine möglicherweise unbefugte Verarbeitung der Daten beim Auftraggeber technisch weitgehend ausschließen dürfte. Daraufhin hat sich das TLS dafür entschieden, nur den Druck und Versand der Erhebungsbögen zu beauftragen und die Belegung im TLS mit eigenen Mitteln zu bewerkstelligen.

Klärungsbedarf bestand bei der Übermittlung der für die Haushaltebefragung auf Stichprobenbasis im Zensus 2011 benötigten Adressen hinsichtlich des Umgangs mit Anschriften aus Meldedatensätzen mit eingetragenen Übermittlungssperren nach § 21 Abs. 5 Melderechtsrahmengesetz (MRRG). Das Zensusgesetz 2011 (§ 3 Abs. 1 Nr. 26) sieht im Unterschied zum Volkszählungsgesetz 1987 vor, dass ausdrücklich auch Melderegistersperren nebst Grund der Übermittlungssperre zu übermitteln sind. Aus statistischen Gründen kam aber beim Zensus 2011 eine Herausnahme dieser Adressen mit Übermittlungssperren nicht in Betracht. Der TLfD hat eine Kompromiss-Lösung mitgetragen, nach der auch diese Adressen in die Haushaltebefragung einbezogen wurden, das TLS aber die Erhebungsbeauftragten (Interviewer) mittels Schulung belehrt hat, bei der Haushaltebefragungen die Auskunftspflichtigen vor der Befragung auf die Möglichkeit einer Selbst- bzw. Online-Ausfüllung des Erhebungsbogens hinzuweisen. Zudem wurden die Auskunftspflichtigen seitens des TLS mittels Ankündigungsschreiben zur Haushaltebefragung über diese Möglichkeiten informiert. Das TIM hatte dem TLfD darüber hinaus zugesichert, zumindest die Betroffenen, denen die Meldebehörde von Amts wegen eine Auskunftssperre im Melderegister einzutragen hatte, per Informationsschreiben hinsichtlich des Zensus 2011, der möglichen Einbeziehung in eine Haushaltebefragung und der genannten Möglichkeiten der Selbstauskunft in Kenntnis zu setzen.

Im Vorfeld des Zensus erfolgten durch den TLfD – auch zur Klärung einer vorliegenden Beschwerde – mehrere Kontrollen bei den Erhebungsstellen. Die gemäß § 6 Abs. 4 ThürAGZensG 2011 erforderlichen Maßnahmen zur Durchführung des Zensus 2011 waren jeweils in einer „Dienstanweisung über die Organisation und Durchführung des Zensus 2011“, die alle personellen, räumlichen, organisatorischen, rechtlichen und sicherheitsrelevanten Fragen für die örtlichen

Erhebungsstellen im Zusammenhang mit der Durchführung des Zensus 2011 regelt, enthalten. Diese wurde dem TLfD jeweils vorgelegt und in den Erhebungsstellen die Umsetzung überprüft. Anlass zur Kritik gab es vor Ort nicht. An der Erstellung dieser Dienstanweisung war der TLfD vorab auf Bitten des TLS auch beratend und datenschutzrechtlich bewertend beteiligt. Sie wurde den Erhebungsstellen sodann seitens des TLS als Muster zur Verfügung gestellt.

Im vorliegenden Beschwerdefall hatte der Beschwerdeführer dem TLfD dargelegt, dass er im Auswahlverfahren der Erhebungsbeauftragten – nach seiner Vermutung – infolge einer unzulässigen Datenübermittlung der Stadtverwaltung Jena an die Erhebungsstelle nicht berücksichtigt worden war. Nach Angaben der zuständigen Gesprächspartner der Erhebungsstelle Jena vor Ort hatte sich der Beschwerdeführer für die Aufgabe „Erhebungsbeauftragter Zensus 2011“ beworben. Seine Ablehnung erfolgte jedoch, weil die nach Auffassung der Erhebungsstelle besser geeigneten anderen Bewerber für das Amt des Erhebungsbeauftragten bei der Auswahl vorgezogen wurden. Bei der großen Anzahl der Bewerber musste eine Auswahl getroffen werden. Aufgabe der Erhebungsstellen ist es gemäß § 9 Abs. 1 ThürAGZens2011 u. a., die benötigten Erhebungsbeauftragten anzuwerben und auszuwählen. Für die Auswahl gilt § 11 Abs. 3 Satz 3 und 4 Zensusgesetz 2011, nachdem i. V. m. § 14 Bundesstatistikgesetz die möglichen Erhebungsbeauftragten von Seiten der Erhebungsstelle hinsichtlich ihrer Zuverlässigkeit, Verschwiegenheit und sonstigen Eignung (nicht unmittelbar in Wohnortnähe, kein Vorliegen von Interessenkonflikten zur beruflichen Tätigkeit usw.) auszuwählen sind. Einen Rechtsanspruch auf den Einsatz als Erhebungsbeauftragter gibt es nicht. Zusammenfassend hat der TLfD nach Prüfung keine Verletzung der Bestimmungen des ThürDSG und anderer Rechtsvorschriften über den Datenschutz in der Angelegenheit feststellen können.

In einem anderen Beschwerdefall wurde dem TLfD mitgeteilt, dass der Beschwerdeführer alleiniger Eigentümer einer Immobilie in einer Stadt in Thüringen sei, er im Rahmen des Zensus 2011 aber ein an ihn und seine Ehefrau gerichtetes Schreiben mit dem Fragebogen „Vorbereitung der Gebäude- und Wohnungszählung 2011“ vom TLS bezüglich dieser Immobilie erhalten habe und dies als eklatanten Datenschutzverstoß ansehe, da seine Ehefrau von der genannten Immobilie nichts wisse. In Frage stand nunmehr, aus welchen

Gründen das Vorerhebungsschreiben des TLS mit der Bitte um Rückmeldung sowohl an ihn als auch seine Frau adressiert worden war. Nach einer Überprüfung durch das TLS wurde von dort eingeräumt, dass es offenbar zu einer manuellen Fehlzuordnung der Adresse bzgl. der in Rede stehenden Immobilie bei der Prüfung des Datenbestandes im länderübergreifenden Erhebungsunterstützungssystem gekommen sei. In Anbetracht der großen Anzahl von zu bearbeitenden Datensätzen sei es nach Mitteilung des TLS trotz hoher Sorgfalt, bedingt auch durch die Vielzahl der Kombinationsmöglichkeiten von Vor- und Familiennamen bei mehreren Immobilien in diesem Einzelfall zu einem Missverständnis gekommen. Nach datenschutzrechtlicher Prüfung der Angelegenheit ist der TLfD davon ausgegangen, dass es sich hier um einen Fehler in einem Einzelfall handelt, der auch bei größter Sorgfalt nicht gänzlich ausgeschlossen werden kann. Der TLfD hat das TLS aufgefordert, seine Mitarbeiter darauf hinzuweisen, bei ähnlichen Konstellationen noch mehr darauf zu achten, dass bei manueller Übertragung der Adressen in die Auskunftsbögen keine Übertragungsfehler unterlaufen.

Der TLfD wird den Zensus 2011 weiter datenschutzrechtlich begleiten.

3 Europäischer und Internationaler Datenschutz

3.1 Gesamtkonzept für den Datenschutz in der Europäischen Union

Bereits seit einigen Jahren hat es sich abgezeichnet, dass in der Europäischen Union nach Wegfall der Säulenstruktur mit dem Vertrag von Lissabon auch ein Gesamtkonzept für den Datenschutz notwendig werden wird. Die EU-Kommission hat in einer Mitteilung vom 4. November 2010 (KOM(2010)609) ihre Vorstellungen veröffentlicht und ein Konsultationsverfahren hierzu eingeleitet. Der BfDI hat in einer mit den Landesbeauftragten abgestimmten Stellungnahme eine Vielzahl von Modernisierungsschritten, u. a. auch aus dem Eckpunktepapier (vgl. 2.1), vorgeschlagen. Eine Modernisierung der Datenschutzrichtlinie aus dem Jahr 1995 ist sicherlich angesichts der seither zu beobachtenden technischen Entwicklung erforderlich. Aus deutscher Sicht ist eine solche Überarbeitung jedoch nicht ohne Risiken. Den am 25. Januar 2012 vorgelegten Entwürfen ist zu entnehmen, dass zwei unterschiedliche Rechtsakte zum Datenschutz angestrebt werden. Die Datenschutzrichtlinie 95/46/EG soll durch eine Verordnung auf der Grundlage des Artikel 16 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) ersetzt werden. Die dort festgelegten Regelungen würden dann nach Artikel 288 AEUV in allen ihren Teilen unmittelbar und verbindlich in allen Mitgliedsstaaten gelten. Das wäre aus Sicht der europaweit tätigen Wirtschaftsunternehmen sicherlich erstrebenswert, da in diesem Fall ein einheitliches Datenschutzniveau anwendbar wäre. Gerade hier könnten sich aber Probleme aus deutscher Sicht ergeben. Traditionell besteht im deutschen Datenschutzrecht ein relativ hohes Schutzniveau für den Umgang mit personenbezogenen Daten. In anderen Mitgliedsstaaten besteht trotz der Harmonisierungspflicht nach der EG-Datenschutzrichtlinie zum Teil ein niedrigeres Datenschutzniveau oder zumindest die Neigung, ein solches künftig festzuschreiben. Bei den anstehenden Verhandlungen über den Kommissionsvorschlag besteht daher die Gefahr, dass die geplante Verordnung ein Datenschutzniveau unterhalb des deutschen Levels festlegt. Eine solche unmittelbare Geltung des EU-Rechts soll es im Bereich der ehemaligen sogenannten Dritten Säule, also der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, nicht geben. Hier hat die EU-Kommission den Entwurf einer Richtlinie vorgelegt,

der allerdings anders als der Rahmenbeschluss 2008/977/JI nicht nur für den Datenaustausch, sondern im Grundsatz auch für innerstaatliche Datenverarbeitungen gelten soll. Insoweit müssen die Mitgliedsstaaten in diesem Bereich die Regelungen im nationalen Recht noch umsetzen. Aber auch hier besteht nach einem jüngsten Urteil des EuGH die Gefahr, dass eine neue Regelung zur Absenkung des deutschen Datenschutzniveaus führen könnte. In seinem Urteil vom 24. November 2011 (Az.: C-468/10) hat der EuGH in Bezug auf die EG-Datenschutzrichtlinie entschieden, dass diese nicht nur einen Mindestdatenschutzstandard vorgibt, sondern auch einen Höchststandard. Sollte dies auch für die künftige Richtlinie im Polizei- und Justizbereich gelten, dann wäre Deutschland gehindert, strengere Datenschutzregeln als in der Richtlinie zu erlassen. Es ist aber jetzt schon klar, dass diese Rechtsakte ganz zentralen Einfluss auf das Datenschutzrecht in Deutschland haben werden.

Eine Modernisierung und Harmonisierung des Datenschutzrechts in Europa ist zu begrüßen, allerdings muss darauf geachtet werden, dass dies nicht auf einem zu niedrigen Niveau erfolgt.

3.2 Keine Vorratsdatenspeicherung und Rasterung von Flugpassagierdaten!

Ein im Jahr 2007 von der EU-Kommission vorgeschlagener Rahmenbeschluss zur Verwendung von Fluggastdatensätzen (PNR-Daten) zur Bekämpfung des Terrorismus und der organisierten Kriminalität (vgl. 8. TB, 3.1) wurde bis zum Inkrafttreten des Vertrages von Lissabon am 1. Dezember 2009 nicht verabschiedet und war damit hinfällig. Die EU-Kommission legte Anfang 2011 den Entwurf einer Richtlinie zur Verwendung von Fluggastdatensätzen zur Gefahrenabwehr und Verfolgung von Straftaten vor, in dem der erreichte Verhandlungsstand des Rahmenbeschlussentwurfes enthalten war. Das zentrale datenschutzrechtliche Problem war aber auch damit nicht gelöst. Nach wie vor sollen von allen Fluggästen, die die EU-Außengrenzen überqueren, aus den Buchungssystemen der Fluggesellschaften ohne Anlass eine Vielzahl von Angaben (z. B. Name, Adresse, Mobiltelefonnummern, Kreditkartendaten, Reisedaten, persönliche Vorlieben während des Aufenthalts im Flugzeug) an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und dort regelmäßig fünf Jahre auf Vorrat gespeichert werden. Bislang

konnte nicht schlüssig nachgewiesen werden, dass eine derartig umfangreiche Datensammlung ohne den geringsten Verdacht für etwaige Straftaten notwendig und verhältnismäßig sein könnte. Das hat auch der Bundesrat in einer Stellungnahme vom 18. März 2011 so gesehen und erhebliche Bedenken gegen den Entwurf geltend gemacht. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer EntschlieÙung (Anlage 16) diese Kritik aufgegriffen und die Bundesregierung und den Bundesrat aufgefordert, sich dafür einzusetzen, dass der Richtlinienvorschlag nicht realisiert wird. Bis zum Redaktionsschluss war die Richtlinie noch nicht erlassen worden.

Da bei diesem Vorschlag auch das Europäische Parlament zu beteiligen ist, könnte dieses möglicherweise dafür sorgen, dass die Grundrechte der Unionsbürger nicht unverhältnismäßig eingeschränkt werden.

3.3 Defizite bei der Umsetzung des SWIFT-Abkommens

Nachdem das Europäische Parlament das Ende 2009 ausgehandelte SWIFT-Abkommen zwischen der EU und den USA zum Zugriff auf Finanztransaktionsdaten zur Terrorbekämpfung u. a. aus Datenschutzgründen im Februar 2010 endgültig abgelehnt hatte (vgl. 8. TB, 3.5), wurde innerhalb weniger Monate ein neues Abkommen ausgehandelt, das zum 1. August 2010 in Kraft getreten ist. Darin wird u. a. Europol eine datenschutzrechtliche Prüffunktion vor der Übermittlung von Daten an die USA eingeräumt. So soll Europol prüfen, ob die von den USA an SWIFT gerichteten Ersuchen zur Übermittlung von Finanzdaten den Vorgaben und Beschränkungen des Abkommens entsprechen. Europol darf zur Durchführung der Prüfungen ergänzende Unterlagen von den US-Behörden anfordern. Dabei ist problematisch, dass Europol bei dieser Prüfung einem Interessenkonflikt unterliegt. So hat Europol in vielen Fällen ebenfalls ein Interesse am Zugriff auf die von den USA begehrten Finanzdaten, kann auf diese aber unter normalen Umständen nicht zugreifen. Können die US-Behörden im Rahmen des Abkommens auf diese Daten zugreifen, so besteht auch für Europol die Möglichkeit, seinerseits von den USA diese Daten zu erhalten. Deshalb besteht Grund zu der Annahme, dass die eigentlich beabsichtigte Kontrollfunktion von Europol nur ein Feigenblatt darstellt oder sogar

in ihr Gegenteil umschlägt. Ein Bericht der Gemeinsamen Kontrollinstanz (GKI), die die datenschutzrechtliche Kontrolle über die Tätigkeit von Europol ausübt, vom Herbst 2011 ließ in dieser Hinsicht nichts Gutes vermuten. Danach war festzustellen, dass Europol jeden eingegangenen Antrag der US-Behörden genehmigt hat, obwohl die schriftlichen Anträge zu allgemein und zu abstrakt formuliert waren, um eine korrekte Bewertung der Notwendigkeit der beantragten Datenübermittlungen vornehmen zu können. Offenbar wurden dabei bewusst Methoden angewandt, die eine Datenschutzkontrolle erschweren. So haben die US-Behörden bestimmten Europol-Bediensteten ergänzende Auskünfte zur Erforderlichkeit der Daten nur unter der Bedingung gegeben, dass keine schriftlichen Aufzeichnungen gemacht werden. Auch hat Europol wenige Tage vor der Kontrolle durch die GKI die US-Ersuchen und alle damit zusammenhängenden Unterlagen als „Geheim“ eingestuft. Damit darf zu konkreten Feststellungen und Ergebnissen dieser Kontrolle nicht öffentlich berichtet werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Missstände zum Anlass genommen, in einer Entschließung (Anlage 17) die politisch Verantwortlichen auf europäischer und nationaler Ebene aufzufordern, die Mängel umgehend zu beseitigen.

Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar.

4 Neue Medien – Rundfunk – Telekommunikation

4.1 Einsatz von Webanalyseprogrammen auf Behördenseiten

Schon im 8. Tätigkeitsbericht wurde unter 15.3 über Web Analytics – auch Web Tracking genannt – berichtet. Dass Nutzung und Erfolg einer Website gemessen werden sollten, ist unbestritten, doch dürfen Nutzungsprofile von Besuchern von Web-Seiten nur unter einem Pseudonym erstellt werden. Die IP-Adresse ist ausdrücklich kein solches Pseudonym. Die aus den Analyseprogrammen gewonnenen Webstatistiken sollen vor allem Ergebnisse zur Anzahl der Besucher einer Webseite bringen und Informationen darüber geben, über welche Wege sie zur eigenen Webpräsenz gelangten. Gemäß § 15 Abs. 3 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Bei Webstatistiken ist Google mit seinem Produkt Google Analytics Marktführer in Deutschland, welches auch von Thüringer Kommunen eingesetzt wird. Da durch das Setzen von Cookies (siehe auch 14.4) unter der Domäne der Webpräsenz und den Google bekannten Merkmalen, wie der IP-Adresse, dem genutzten Browser und die Zeit des Seitenaufrufes die Möglichkeit besteht, ein übergreifendes Bewegungsprofil zu erstellen, wurde der Einsatz von Google Analytics in öffentlichen Stellen von den Datenschutzbeauftragten des Bundes und der Länder als sehr kritisch gesehen. Im Ergebnis der Gespräche des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit mit Google Deutschland bekannte sich im September 2011 Google Deutschland zur datenschutzkonformen Ausgestaltung von Google Analytics. Im Verfahren ist nun die Löschung des letzten Oktetts der IP-Adresse und ein Widerspruch gegen die Erfassung von Nutzungsdaten mittels eines von Google bereit gestellten Deaktivierungs-Add-On durch den Nutzer möglich. Neben diesen zwei umzusetzenden Parametern, muss der Webseitenbetreiber, um einen datenschutzgerechten Betrieb von Google Analytics zu ermöglichen,

zudem schriftlich einen Vertrag zur Auftragsdatenverarbeitung abschließen.

Informationen zu diesem Vertrag stehen unter <http://www.google.de/intl/de/analytics/tos.pdf> zum Abruf bereit. Dieser Vertrag entlastet die Behörden aber nicht von ihrer Kontrollpflicht. Ein weiteres Produkt zur Webanalyse ist bspw. das Programm Piwik. Der Vorteil von Piwik ist, dass es auf dem Webserver des Anwenders installiert wird und somit alle erfassten Daten auf dem Server verbleiben. Durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) wurde das Programm Piwik analysiert und bei datenschutzkonformer Implementierung als eine mögliche Alternative zur datenschutzrechtlich unzulässigen Anwendung anderer Analysedienste gesehen (<http://www.datenschutzzentrum.de>).

Behörden, die Webseitenanalyseprogramme einsetzen, sollten überprüfen, inwieweit diese datenschutzgerecht implementiert sind.

4.2 IPv6: Datenschutz ins Netz einbauen!

Computer erkennen sich im Internet untereinander mithilfe der sogenannten IP-Adressen. Das hierzu bislang verwendete Internet-Protokoll Version 4 (IPv4) ist nun an Kapazitätsgrenzen gestoßen.

Das Internet-Protokoll Version 6 (IPv6) befindet sich in der Phase der Einführung in die zurzeit noch mit IPv4 betriebenen Netzstrukturen, darunter das Internet. Die letzten freien Adressen von IPv4 sind vergeben, der durch die 32-Bit-Struktur (4 Gruppen zu je 8 Bit, dezimal codiert, z. B. 192.185.154.13) vorgegebene Adressraum mit 4.294.967.296 physischen Adressen ist ausgeschöpft. Webseiten-Betreiber sind auf feste IP-Adressen angewiesen. Wenn keine festen IP-Adressen mehr verfügbar sind, können keine neuen Webseiten mehr veröffentlicht werden. Zumindest bei den Internetunternehmen wird das Jahr 2012 das Jahr der Umstellung auf IPv6 werden. Im privaten Bereich wird sich IPv4 sicherlich noch eine Weile halten, zumal die Umstellung meist auch neue Hardware voraussetzt.

Eine IPv6 Adresse „2001:0db8:85a3:08d3:1319:8a2e:0370:7344“, besteht aus acht Hextets und könnte bspw. die Adresse eines Endgerätes, etwa eines iPad sein. Ein 128 Bit Binärcode, hexadezimal codiert, ermöglicht 340 Sextillionen Adressen wie die oben genannte. Das entspräche 600 Billiarden Adressen auf jeden Quadratmilli-

meter der Erdoberfläche. Server, Router, Handys und Computer müssen über die notwendigen Hardwarevoraussetzungen verfügen und entsprechend programmiert werden, damit sie mit dem IPv6-Protokoll umgehen können.

Am 8. Juni 2011, dem sogenannten IPv6-Day, wurde erstmals in größerem Maßstab im Internet der Betrieb von Webseiten zusätzlich mit dem IPv6-Protokoll getestet. Unternehmen wollten vor dem weltweiten Start noch die letzten Probleme aufspüren. Noch sind nicht alle auf dem Markt verfügbaren Geräte IPv6 kompatibel. Die Umstellung erfordert Austausch von Komponenten und teilweise Neustrukturierung von logistischem Beiwerk im Internet. Damit der Adressenexplosion praktisch jedes am Netzwerkverbund teilhabende Individuum und sogar jedes seiner „Geräte“ eine eigene öffentliche Adresse erhalten könnte und somit auf „Lebzeiten“ eindeutig identifizierbar bliebe, kommt den Fragen des Datenschutzes eine besondere Wichtigkeit zu. Ein totaler Anonymitätsverlust im Internet wäre theoretisch möglich. Von jeder Person wäre bekannt, auf welcher Website sie gerade surft, ob sie dies von ihrem Handy oder Computer aus tut und ob sie vielleicht gerade mit ihrem Kühlschrank kommuniziert. Der "gläserne Mensch" mit Datenschutzlevel „zero“ wäre realisierbar. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Arbeitsgruppe eingesetzt, die untersuchen soll, welche konkreten Folgen der Einsatz von IPv6 für den Datenschutz hat und welche Empfehlungen daraus abzuleiten sind. Es gibt aber nicht nur Risiken, sondern auch Chancen. So wäre eine echte Peer-to-Peer-Kommunikation (P2P) nach dem Ende-zu-Ende-Prinzip ohne zwischengeschaltete Provider möglich. Lediglich die Endknoten führten dann aktive Protokolloperationen aus, das Netz wäre „nur noch“ Vermittler. Da jeder Nutzer dauerhaft über dieselbe IP-Adresse erreichbar wäre, könnte sogar eine Ende-zu-Ende-Verschlüsselung z. B. bei E-Mail oder VPN erfolgen. Keinesfalls sollte anstelle einer neuen Internet-Welt ein "Register der Internetnutzer" und damit das Ende der Anonymität entstehen.

Damit es nicht soweit kommt, haben Internetprovider angekündigt, auch bei IPv6 dafür zu sorgen, dass die IP-Adresse bei jedem Einwählen ins Internet neu vergeben wird (Dynamisierung). Abhilfe versprechen auch die sogenannten „Privacy Extensions“. Ein Teil

der IP-Adresse – der Interface-Identifier – wird dabei bspw. durch einen Hash-Code ersetzt und somit „verschleiert“, sodass weitgehend anonym gesurft werden kann. Diese Privacy Extensions sollten für jedes internetfähige Gerät herstellerseitig zur Pflicht werden, um ein ausreichendes Datenschutzniveau auch bei IPv6 zu erhalten.

Für die Umsetzung eines ausreichenden Datenschutzniveaus bei der Einführung des IPv6-Protokolls fassten die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 82. Konferenz eine Entschlieung (Anlage 25), die sich an Betreiber und Anwender ffentlicher Netzwerke sowie Hersteller von Netzwerkkomponenten richtet. IPv6 darf nicht zu einer Verschlechterung des Datenschutzniveaus fhren. Zu den Forderungen gehrt u. a. dass fr den Einsatz datenschutzgerechter Technologien mageblich die Anbieter von Diensten (Provider) und die Hersteller der Produkte („Privacy by design“) verantwortlich sind. Bereits bei der Auslieferung neuer Gerte sollten datenschutzgerechte Lsungen („Privacy Extensions“) verwendet und voreingestellt werden („Privacy by default“). Geolokalisation und Reichweitenanalysen sind mit den ersten 4 Byte der IPv6-Adresse mglich, sodass der Rest der Adresse zu lschen ist.

Die Einfhrung von IPv6 wird weiterhin wachsam beobachtet, wobei die Datenschutzbeauftragten allen Akteuren ihre Untersttzung fr datenschutzgerechte Lsungen anbieten.

4.3 Chance zum datensparsamen Rundfunkgebhreneinzug verpasst

Bereits im Oktober 2000 forderten die Datenschutzbeauftragten des Bundes und der Lnder auf ihrer 60. Konferenz die Bundeslnder auf, bei der Rundfunkfinanzierung zuknftig ein Modell zu Grunde zu legen, das sich strker als das bestehende System an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert (4. TB, Anlage 9). Gegenstand der ffentlichen Diskussion war damals der 6. Rundfunknderungsstaatsvertrag. Erst im Dezember 2010, also zehn Jahre spter, wurde im 15. Rundfunknderungsstaatsvertrag ein Modellwechsel vom gerteabhngigen zum haushalts- und betriebsstttenbezogenen Rundfunkbeitrag verankert. Doch wieder sind die Datenschutzbeauftragten unzufrieden. Schlielich erffnete dieser 15. Rundfunknderungsstaats-

vertrag die Möglichkeit, ab 2013 nicht nur das Modell zu wechseln, sondern auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug – jetzt Beitragseinzug – auf das erforderliche Maß zu begrenzen. Da der Entwurf des 15. Rundfunkänderungsstaatsvertrages dem nicht entsprach, forderten die Datenschutzbeauftragten des Bundes und der Länder im Oktober 2010 erneut die Staatskanzleien auf, noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit den Entwurf nachzubessern (Anlage 7). Trotz dieser Empfehlungen der Datenschutzbeauftragten wurde auf der Ministerpräsidentenkonferenz im Dezember 2010 der jetzt vorliegende Staatsvertrag von den Regierungschefs unterzeichnet und zur Zustimmung in die Länderparlamente überwiesen. Die Chance zum datensparsamen Beitragseinzug wurde somit verpasst.

Im Juni 2011 legte die Thüringer Landeregierung einen entsprechenden Gesetzentwurf zum „Thüringer Gesetz zur Neuordnung der Rundfunkfinanzierung“ vor, welcher in Artikel 1 das Gesetz zum 15. Rundfunkänderungsstaatsvertrag beinhaltet.

Ende September 2011 bat der u. a. für Medien zuständige Europaausschuss des TLT im schriftlichen Anhörungsverfahren den TLfD hierzu um eine Stellungnahme. Vom Grundsatz her befürwortete der TLfD eine Neuordnung der Rundfunkfinanzierung, eine Zustimmung zum vorliegenden Staatsvertrag in der aktuellen Ausgestaltung wurde allerdings nicht empfohlen. Die datenschutzrechtlichen Bedenken blieben weitgehend erhalten, da die Erhebungsbefugnisse im 15. Rundfunkänderungsstaatsvertrag teilweise ausgeweitet und zusätzlich durch weitere Rechtfertigungstatbestände ergänzt wurden. Die für die Landesrundfunkanstalt bspw. geplanten nicht klar definierten Erhebungs- und Verarbeitungsvorschriften, die Möglichkeit, Dritte tätig werden zu lassen, ungeprüfte Adressdaten von nicht-öffentlichen Stellen einzukaufen und nicht geprüfte Daten bis zu 12 Monate vorzuhalten, widersprechen weiterhin dem Prinzip der Datenvermeidung und Datensparsamkeit sowie Normenklarheit und Transparenz. Trotzdem verabschiedete der TLT in seiner 69. Sitzung am 16. November 2011 das Thüringer Gesetz zur Neuordnung der Rundfunkfinanzierung und somit den 15. Rundfunkänderungsstaatsvertrag ohne Änderungen. Die Bedenken des TLfD wurden allerdings zum Teil in dem vom TLT gefassten Beschluss „Modellwechsel zukunftssicher gestalten“ aufgegriffen. So erwartet der TLT

u. a., dass die Datenerhebungsbefugnisse beim Beitragseinzug auf das erforderliche Maß beschränkt werden und die Lösungsfristen für nicht oder nicht mehr benötigte Daten so kurz wie möglich gehalten werden müssen. Auch sollte nach Ansicht des TLT, um einen datenschutzrechtskonformen Umgang mit den übermittelten Daten zu überprüfen, zeitnah eine Evaluierung von unabhängiger Seite durchgeführt werden (Landtagsdrucksache 5/3572). Der TLfD hofft nun, dass seine Vorschläge und die diesbezüglichen Forderungen des TLT in einer möglichen Satzung der Landesrundfunkanstalt Berücksichtigung finden. Die zuständigen Landesrundfunkanstalten sind gemäß § 9 Rundfunkänderungsstaatsvertrag ermächtigt, Einzelheiten des Verfahrens durch Satzung zu regeln. Die Satzung bedarf der Genehmigung der für die Rechtsaufsicht zuständigen Behörde und soll laut Staatsvertrag mit den Satzungen der anderen Landesrundfunkanstalten übereinstimmen.

Der Empfehlung des TLfD gegenüber dem TLT, der Neuordnung der Rundfunkfinanzierung in der aktuellen Ausgestaltung nicht zuzustimmen, wurde nicht entsprochen. Um Einzelheiten des Verfahrens wie gefordert datenschutzgerechter zu regeln, sollte nun die Möglichkeit einer Satzung durch die Landesrundfunkanstalt genutzt werden. Der TLfD bietet hierfür seine Unterstützung an.

4.4 Notrufortung von Mobilfunkteilnehmern durch Rettungsleitstellen

Gemäß § 30 Abs. 1 Thüringer Rettungsdienstgesetz (ThürRettG) gelten für alle in Thüringen am Rettungsdienst beteiligten Stellen die Bestimmungen des ThürDSG, soweit sich aus dem ThürRettG nichts anderes ergibt. Dies gilt somit auch für die Notrufortung durch öffentliche Stellen oder im Auftrag der öffentlichen Stellen. Anfang 2011 wandte sich der Rettungsdienstzweckverband Südthüringen an den TLfD mit der Anfrage, ob es hinsichtlich eines Vertrages mit der Allianz OrtungsServices GmbH (AOS) Stuttgart Bedenken gibt, deren Dienst zur Notfallortung genutzt werden soll. Der TLfD wies wie der BfDI darauf hin, dass derzeit gegen eine Übermittlung (Abruf) von Standortdaten von Notrufenden an die Notrufzentralen durch den Netzbetreiber unter Verwendung der Plattform der AOS auf der Basis einer Auftragsdatenverarbeitung nach § 11 BDSG keine Bedenken bestehen. Die Ermittlung der Standort-

daten bei dem jeweiligen kooperierenden Mobilfunknetzbetreiber und die Übermittlung dieser Daten an die jeweilige Rettungsleitstelle erfolgt gemäß § 108 Abs. 1 Satz 2 TKG. Die AOS als Auftragnehmerin für die Mobilfunknetzbetreiber verfügt hierzu über ein internetgestütztes Softwaresystem, welches unter bestimmten Voraussetzungen eine Standortbestimmung von Mobilfunkendgeräten sowie – im Falle des sogenannten eCalls – von Kraftfahrzeugen ermöglicht („Ortungsplattform“). Zusätzlich ist bei GPS-fähigen Endgeräten die Ortung auch über GPS möglich. Da zwecks Abruf von Standortdaten zu einem Mobilfunkgerät oder einem Kraftfahrzeug der Rettungsleitstelle ein Zugriff auf die Ortungsplattform eingerichtet wird, wies der TLfD darauf hin, dass eine Verwendung der Plattform für andere Zwecke, etwa für eine Ortung im Rahmen einer Gefahrenabwehr nach Landesrecht ausscheidet, da hierfür abschließende Regelungen im Thüringer Polizeiaufgabengesetz zur Verwendung von Standortdaten eines Mobilfunkendgeräts vorliegen. Ergänzend sollte in der Rettungsleitstelle eine Protokollierung der Abfragen vorgenommen werden, um ggf. Missbrauch der Ortungsmöglichkeit nachträglich feststellbar zu machen. Hier sollten angemessene Aufbewahrungsfristen festgelegt werden.

Da seit Juni 2011 die von der Bundesnetzagentur veröffentlichte technische Richtlinie Notrufverbindungen (TR Notruf) u. a. die neue Übertragungstechnik bei Notfallortung regelt, die bis Ende 2012 funktionsfähig implementiert sein muss, ist diese Auftragsdatenverarbeitung allerdings in ca. einem Jahr von dem Rettungsdienstzweckverband Südthüringen auf Erforderlichkeit zu überprüfen. Gemäß dieser TR Notruf hat der Telefondiensteanbieter (Anbieter des öffentlich zugänglichen Telefondienstes) beim Verbindungsaufbau die geografische Rufnummer, nationale Teilnehmerrufnummer oder Mobilfunkrufnummer des Anschlusses, von dem die Notrufverbindung ausgeht, auch wenn die Rufnummernanzeige unterdrückt ist, zu übertragen. Bei der Ermittlung des Standortes des Notrufenden hat dann auch der Telefondiensteanbieter die geografischen Koordinaten zu übermitteln. Bei Festnetzanschlüssen kann anstatt der geografischen Koordinaten des Standortes des Endgerätes die amtliche Anschrift (Postleitzahl, Straßename und Hausnummer) des Installationsortes angegeben werden. Für Mobilfunkanschlüsse ist der Standort des Endgerätes zum Zeitpunkt des Erkennens des Verbindungswunsches des Notrufenden zu ermitteln. Verfügt der Telefondiensteanbieter nicht über die aktuellen Standortdaten des

Endgerätes des Notrufenden, so hat er, gemäß der TR Notruf, den vom Telekommunikationsnetz festgelegten Standort des Endgerätes beim Erbringer von Vorleistungen unverzüglich zu ermitteln. Der Telefondiensteanbieter hat die notrufbegleitenden Informationen und die Nummer des Notrufanschlusses zum ermittelten Notrufursprungsbereich entweder direkt an das Zielnetz oder an das Transitnetz, welches für den öffentlich zugänglichen Telefondienst geeignet ist und den weiteren Verbindungsaufbau einschließlich der unveränderten Weitergabe der notrufbegleitenden Informationen zum Zielnetz erledigt, zu übertragen. Diese Übertragungstechnik soll eben spätestens 18 Monate nach Inkrafttreten der TR Notruf umgesetzt sein. Maßnahmen, die zur Sicherung der technischen Schnittstellen gegen Missbrauch erforderlich sind, sollen allerdings nach Angaben der Bundesnetzagentur erst in einer künftigen TR Notruf festgelegt werden. Sind diese gesetzlichen Vorgaben erfüllt, dann entfällt bereits die Erforderlichkeit einer Dienstleistung durch die Allianz OrtungsService GmbH.

Auch bei Notfallortung muss die datenschutzgerechte Verarbeitung der erhobenen Daten gewährleistet sein.

Zur Sicherung der technischen Schnittstelle bei Notfallortung erwartet der TLfD von der Bundesnetzagentur, zeitnah die angekündigten erforderlichen Maßnahmen gegen Missbrauch der Daten festzulegen.

5 Kommunales

5.1 Ergebnisse der Kommunalkontrollen

Im 8. Tätigkeitsbericht (5.1) hatte der TLfD über die Kontrolle des Grunddatenschutzes in 40 Kommunalverwaltungen berichtet. Die damaligen Niveauunterschiede wurden auch bei der Erledigung der datenschutzrechtlichen Forderungen bestätigt. So sind es meist die kleinen Gemeinden, die sich mit der Herstellung des rechtskonformen Zustandes schwer tun. Im Nachgang zu den Kontrollen wurden fünf Kommunen nochmals beanstandet, da sie ihrer Verpflichtung, den TLfD gemäß § 38 ThürDSG in der Erfüllung seiner Aufgaben zu unterstützen, nur unzureichend nachgekommen waren. Das betraf die VG Heldburger Unterland sowie die Städte Schkölen, Kahla, Stadtlengsfeld und Ruhla. Schwierig gestaltet sich die Erarbeitung von auf die Bedingungen der jeweiligen Verwaltungen zugeschnittenen Sicherheitskonzepten nach § 9 ThürDSG. Ein gutes Hilfsmittel zur Festlegung eines Maßnahmenkatalogs sind dabei die im Internet eingestellten Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik.

Zum 31. Dezember 2011 waren die Kontrollverfahren in 23 Kommunen abgeschlossen. In einigen Fällen hat sich der TLfD zu gegebener Zeit Nachkontrollen vorbehalten. Demgegenüber waren 17 Verwaltungen noch nicht allen Forderungen nachgekommen. Darunter befinden sich 13 Kommunen, von denen Anfang des Jahres 2012 eine Erledigung aller offenen Forderungen aus eigener Kraft bzw. mittels externer Dienstleister erwartet werden kann. Problematisch stellt sich die Situation in vier Kommunen dar, darunter je eine Gemeinde unter 3.000, zwischen 3.000 und 10.000 Einwohnern sowie zwei Verwaltungsgemeinschaften.

Es war festzustellen, dass in den Fällen, in denen die zuständige Kommunalaufsichtsbehörde eingeschaltet wurde, die Kommunen von dort aus oft nicht ausreichend angehalten wurden, die datenschutzrechtlichen Vorgaben zu erfüllen. Als Grund wurde die fehlende personelle Kapazität angegeben. Viele Kommunen haben gegenüber dem TLfD Schulungsbedarf angemeldet. Derartige Schulungen kann der TLfD wegen seiner unzureichenden Personalausstattung nur im begrenzten Umfang durchführen. Der TLfD hatte

gegenüber dem TIM und den kommunalen Spitzenverbänden auf den erforderlichen Schulungsbedarf hingewiesen und Unterstützung in Form der Prüfung der Schulungsunterlagen und Teilnahme an einzelnen Veranstaltungen angeboten. Leider wurde diese Initiative nicht in ausreichendem Maße aufgegriffen.

Schulungsangebote öffentlicher und privater Anbieter sind vorhanden und Informationen hierzu sind bei den kommunalen Spitzenverbänden nachzufragen.

Die Herstellung einer datenschutzkonformen Verwaltung ist in der Regel keine kurzfristige Aufgabe. Um einen guten Stand zu erreichen bzw. zu halten ist eine fortlaufende Aktualisierung aller datenschutzrechtlichen Dokumente und Regelungen, insbesondere des Sicherheitskonzepts, erforderlich.

Der Bedarf an datenschutzrechtlichen Schulungen sollte ernster genommen werden. Der TLfD fordert mehr Unterstützung von den Aufsichtsbehörden!

5.2 Veröffentlichungen im Internet durch Kommunen

Bereits im 8. Tätigkeitsbericht (5.3) hatte der TLfD über datenschutzrechtliche Probleme bei der Veröffentlichung kommunaler Dokumente im Internet berichtet. Zahlreiche Anfragen und Beschwerden im darauf folgenden Berichtszeitraum zeigten, dass das Thema nicht an Brisanz eingebüßt hat. Insgesamt ist der Trend zu verzeichnen, dass Kommunen sich in immer stärkerem Maß im Internet präsentieren. Dies ist leider oft mit Verstößen gegen geltendes Datenschutzrecht verbunden:

So war festzustellen, dass jedermann erfolgreich auf der Internetseite der Stadtverwaltung Rudolstadt Dokumente des Stadtrates Rudolstadt recherchieren konnte, die teilweise sensible personenbezogene bzw. personenbeziehbare Daten enthielten.

Ein Beschwerdeführer trug vor, dass er einem Bebauungsplan der Stadtverwaltung Eisenach widersprochen habe. Daraufhin sei anstelle einer persönlichen Antwort sein Widerspruchsschreiben samt seiner Adresse auf der Internetseite der Stadtverwaltung veröffentlicht worden. Zur Ursache des Vorkommnisses teilte die Stadtverwaltung mit, dass die Beschlussvorlage des Amtes für Stadtentwicklung in öffentlicher Stadtratssitzung behandelt worden sei. Der öffentliche Beschluss nebst Anlagen mit dem Widerspruchsschreiben

sei zum Termin der Stadtratssitzung von der Pressestelle ins Internet eingestellt worden, ohne die Unzulässigkeit einer Veröffentlichung der darin enthaltenen personenbezogenen Daten zu beachten.

In einem anderen Fall hatte die Gemeinde Saaleplatte in ihrem, auch im Internet publizierten, Amtsblatt einen Beschluss aus einer nicht-öffentlichen Gemeinderatssitzung zu einem gerichtlichen Vergleich zwischen namentlich genannten Personen und dem Landkreis ohne Einwilligung der Betroffenen veröffentlicht.

Weiterhin wurde bekannt, dass im Amtsblatt der Stadt Brotterode, welches im Internet veröffentlicht wird, die Geburtstagsdaten von Einwohnern veröffentlicht wurden.

Bei einer Internetpublikation personenbezogener Daten handelt es sich um eine Datenübermittlung auch an Drittstaaten nach § 23 Abs. 2 ThürDSG, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Dies ist nur zulässig, wenn die Betroffenen hierin eingewilligt haben und die Datenübermittlung zur Aufgabewahrnehmung durch die Kommunen erforderlich ist. Gegen diese Rechtsauffassung wenden sich sowohl das TLVwA als auch das TIM u. a. mit folgender Argumentation:

Der EuGH hat in der sog. Lindqvist-Entscheidung (Urteil vom 06.11.2003, Az.: C – 101/01) angenommen, dass keine Übermittlung von Daten in ein Drittland i. S. v. Art. 25 der EG-Datenschutzrichtlinie vorliegt, wenn eine sich in einem Mitgliedsstaat aufhaltende Person in eine Internetseite, die bei ihrem in demselben oder einem anderen Mitgliedsstaat ansässigen Provider gespeichert ist, personenbezogene Daten aufnimmt und diese damit jeder Person, auch in Drittländern, zugänglich macht. Dem kann für Thüringen nicht gefolgt werden. Anders als in der EG-Datenschutzrichtlinie findet sich in § 3 Abs. 3 Nr. 4 ThürDSG eine ausdrückliche Definition des Begriffs des „Übermittels“. Übermitteln ist die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte in der Weise, dass die Daten durch die Daten verarbeitende Stelle an den Dritten weitergegeben werden oder der Dritte bei der Daten verarbeitenden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder dort abrufen. Die Definition des ThürDSG umfasst damit ausdrücklich auch das Einstellen in das Internet. Die Übermittlung von Daten findet statt, wenn der Dritte die Daten einsieht oder abrufen.

Weiterhin beruft sich das TIM auf einen Beschluss des Bundesverwaltungsgerichts vom 12.03.2008 (Az.: 2 B 131/07), in welchem

dargelegt wird, dass soweit eine juristische Person des öffentlichen Rechts befugt sei, ihre behördliche und organisatorische Struktur zu regeln, sie auch ohne ausdrückliche gesetzliche Ermächtigung befugt sei, dem außenstehenden Benutzer, für dessen Bedürfnisse sie eingerichtet worden ist, einen Hinweis darauf zu geben, welche natürlichen Personen als Amtswalter (Beamte, Angestellte) mit der Erfüllung einer bestimmten Aufgabe betraut sind. Folgte man dieser Auffassung, würde das bedeuten, dass die Veröffentlichung der Namen der Mitarbeiter einer juristischen Person des öffentlichen Rechts keinen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Eine derartige Rechtsauslegung würde gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen, das „insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ gewährleistet (BVerfG im so genannten Volkszählungsurteil vom 15.12.1983, Az.: 1 BvR 209, 269, 362, 420, 440, 484/83).

Anders stellt sich die Rechtslage bei einer Veröffentlichung im Internet dar. Hierbei handelt es sich aufgrund der Möglichkeit, weltweit Einsicht nehmen zu können, um eine Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes, deren Zulässigkeit sich nach § 23 ThürDSG beurteilt. Die Übermittlung ist darüber nach § 23 Abs. 1 Satz 3 ThürDSG nur zulässig, wenn ein angemessenes Datenschutzniveau gewährleistet ist. Daran fehlt es jedoch regelmäßig, da die Veröffentlichung immer auch in Staaten erfolgt, die kein angemessenes Datenschutzniveau besitzen. Deshalb kann selbst bei dem Vorliegen des Tatbestandsmerkmals der Erforderlichkeit einer Veröffentlichung (Notwendigkeit von Außenkontakten) eine Internetveröffentlichung immer nur mit der Einwilligung des Betroffenen nach § 23 Abs. 2 Nr. 1 ThürDSG erfolgen.

Auf Veranlassung des TLfD wurden die personenbezogenen Daten, die Gegenstand der konkreten datenschutzrechtlichen Prüfung waren, unkenntlich gemacht bzw. aus dem Internet genommen und wurde zugesagt, eine solche Veröffentlichung künftig zu unterlassen oder lediglich in anonymisierter Form vorzunehmen.

Grundsätzlich gehen immer mehr Kommunen dazu über, die Niederschriften Ihrer Sitzungen ins Internet zu stellen und Mitschnitte dieser Sitzungen im Internet zu übertragen.

Wie im 8. Tätigkeitsbericht des TLfD ausführlich dargelegt wurde, begegnet eine Veröffentlichung von Niederschriften auch des öffent-

lichen Teils von Gemeinderatssitzungen sowie von Beschlussvorlagen, die personenbezogene Daten enthalten, im Internet rechtlichen Bedenken, sodass eine datenschutzrechtliche Zulässigkeit zu verneinen ist. Gleiches gilt für Veröffentlichungen von Filmaufnahmen der Ratssitzungen durch die Kommunen im Internet. Allerdings hat der TLfD grundsätzlich Verständnis für das Anliegen der Kommunen, die – dem Gebot der Transparenz folgend – Sitzungsniederschriften oder andere Informationen über Ratssitzungen ins Internet stellen möchten. Die Voraussetzungen hierzu sollten aber gesetzlich geregelt sein. Hierzu hat der TLfD sowohl gegenüber dem TIM als auch im parlamentarischen Anhörungsverfahren zum Gesetz zur Änderung des Thüringer Datenschutzgesetzes und anderer Vorschriften einen Regelungsvorschlag unterbreitet. Leider wurde dieser Vorschlag nicht aufgegriffen. Solange eine entsprechende gesetzliche Regelung nicht existiert, ist die Veröffentlichung von Niederschriften im Internet und die Veröffentlichung von (Live-)Mitschnitten aus Ratssitzungen nur unter den Voraussetzungen des § 23 ThürDSG zulässig.

Die vorliegenden Beschwerden und Anfragen zu Internetpublikationen personenbezogener Daten machen die Brisanz des Problems deutlich. Wünschenswerte Neuregelungen dieser Problematik werden danach zu beurteilen sein, ob sie gewährleisten, dass die gebotene Öffentlichkeit des kommunalen Verwaltungshandelns und der Tätigkeit kommunaler Gremien nicht zu Lasten des Schutzes des informationellen Selbstbestimmungsrechtes der Betroffenen geht. Der TLfD wird die weitere Entwicklung in diesem Bereich kritisch verfolgen.

5.3 Verstöße gegen das Postgeheimnis

Eine Beschwerde betraf einen ehrenamtlichen Bürgermeister einer Mitgliedsgemeinde der Verwaltungsgemeinschaft „An der Marke“, der an Einwohnermeldeamt und Standesamt der VG adressierte Schreiben trotz mehrfacher Hinweise geöffnet und gelesen hatte. Ein ähnlicher Fall hatte den datenschutzkonformen Umgang mit einem

fehlerhaft adressierten Schreiben durch das Landratsamt Hildburghausen zum Thema. Dieses Schreiben war persönlich an den Vorsitzenden eines kommunalen Gremiums unter der Adresse des Landratsamtes gerichtet. Obwohl der Adressat nicht im Landratsamt arbeitete, wurde der Brief dort geöffnet, „um feststellen zu können, welche Wünsche der Bürger hat.“. Der TLfD hat zunächst in beiden Fällen darauf hingewiesen, dass nach § 202 Abs. 1 Nr. 1 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird, wer unbefugt einen verschlossenen Brief oder ein anderes Schriftstück, das nicht zu seiner Kenntnis bestimmt ist, öffnet. Die Beurteilung, ob dieser Straftatbestand erfüllt wurde, fällt in die Zuständigkeit der Strafverfolgungsbehörden. Aus datenschutzrechtlicher Sicht stellt das Öffnen eines Briefes angesichts der konkreten Adressierung ein Erheben von personenbezogenen Daten dar. Das Erheben personenbezogener Daten ist nur dann zulässig, wenn ihre Kenntnis für die Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist, § 19 Abs. 1 ThürDSG. Für das Vorgehen des ehrenamtlichen Bürgermeisters war keine Rechtsgrundlage ersichtlich. Insbesondere ist das Öffnen solcherart adressierter Briefe nicht für die Aufgabenerfüllung eines ehrenamtlichen Bürgermeisters, dem keine Verantwortung für das Einwohnermeldeamt und das Standesamt der Verwaltungsgemeinschaft zukommt, erforderlich. Im Übrigen sind auch die an Behördenmitarbeiter selbst gerichteten Schreiben diesen verschlossen auszuhändigen. Sollte eine direkte Übergabe eines Schreibens an den Adressaten aufgrund einer fehlerhaften oder widersprüchlichen Adressierung nicht mit der gebotenen Sicherheit möglich sein, ist es keinesfalls zu öffnen, sondern an den Absender zurück zu senden, sofern dieser bekannt ist. Dem Absender sollte erläutert werden, warum die Rücksendung erfolgte. Im Ergebnis handelte es sich somit in beiden Fällen um Verstöße gegen das Datenschutzrecht. Beide Behörden wurden darauf hingewiesen, dass entsprechende Regelungen zum Postlauf zu fixieren und allen Mitarbeitern zur Kenntnis zu geben sind. In beiden Fällen wurde nach Auswertung der Angelegenheit eine Dienstanweisung zur Regelung des Postlaufs erstellt.

Klarere Regelungen zum Postlauf, insbesondere zur vertraulichen Behandlung personenbezogener Daten, sind ein unabdingbares organisatorisches Mittel des Datenschutzes.

5.4 Mietwerterhebung unter Mitwirkung privater Dritter oder aus eigener Kraft

Ein Unternehmen bietet Landratsämtern an, eine Mietwerterhebung im Wege der anonymisierten Befragung zur Bestimmung einer angemessenen Höhe der Kosten der Unterkunft nach § 22 SGB II im Rahmen des ALG II unter Nutzung von Kundenadressen des kommunalen Abfallwirtschaftsbetriebs (Abfallwirtschaft) auf der Grundlage einer der beiden nachfolgenden Verfahrensalternativen durchzuführen:

1. Auftragsdatenverarbeitung durch das Unternehmen:

Weitergabe der Adressdaten der Abfallwirtschaft an das Privatunternehmen, das die Mietwerterhebung im Wege einer Auftragsdatenverarbeitung für die Abfallwirtschaft durchführt.

2. Daten- bzw. Adressmittlung:

Das Privatunternehmen verpackt lediglich die Anschreiben. Danach werden die gefüllten Kuverts durch die Abfallwirtschaft mit geeigneten Kundenadressen versehen und an die Teilnehmer der Befragung versandt.

Regelmäßig wird der privatrechtlich organisierte Abfallwirtschaftsbetrieb für die untere Abfallbehörde tätig, weshalb das ThürDSG i. V. m. dem ThürAbfG anzuwenden ist. Nach § 30 Abs. 1 ThürAbfG dürfen Abfallbehörden personenbezogene Daten nur zum Zwecke der Durchführung und Überwachung der Abfallentsorgung, der Abfallwirtschaftsplanung sowie zur Durchführung von Anzeige-, Genehmigungs-, Planfeststellungs- und sonstigen Zulassungsverfahren, die im Zusammenhang mit den vorgenannten Zwecken stehen, erheben, verarbeiten und nutzen. Gemäß § 30 Abs. 6 ThürAbfG bleiben die Bestimmungen des ThürDSG im Übrigen unberührt. Eine Verarbeitung der Adressdaten der Abfallbehörde für andere Zwecke wie die Mietwerterhebung durch einen privaten Dritten (Alternative 1) ist als Verstoß gegen datenschutzrechtliche Bestimmungen anzusehen.

Eine Ermächtigung hierfür ergibt sich nicht aus § 20 Abs. 2 Nr. 3 und 5 ThürDSG, da diese Bestimmung auf die Übermittlung personenbezogener Daten nicht anwendbar ist. Unter Nutzung im Sinne dieser Vorschrift ist nur die Datenverwendung für andere Zwecke der Behörde, nicht jedoch Dritter zu verstehen. Auch § 22 ThürDSG

(Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs) ist nicht einschlägig, da im Sinne dieser Vorschrift die Übermittlung der Kundendaten nicht zur Erfüllung der in der Zuständigkeit der übermittelnden Abfallbehörde liegenden Aufgaben erforderlich ist und auch das die Daten empfangende Privatunternehmen kein schützenswertes berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft machen kann. Zudem haben die Betroffenen hier gerade ein schutzwürdiges Interesse am Ausschluss der Übermittlung. Diese Alternative ist daher als nicht zulässig zu bewerten.

Das Adressmittlungsverfahren (Alternative 2) ist wie folgt zu beurteilen: Hierbei verpackt das beauftragte Privatunternehmen lediglich die Anschreiben bzw. Fragebögen. Danach werden die gefüllten Kuverts durch die öffentliche Stelle mit geeigneten Adressen aus dem eigenen Datenbestand versehen und an die Teilnehmer der Befragung versandt. Es sollte auch bei der Gestaltung der Rücksendung dafür Sorge getragen werden, dass die Anschrift des Absenders dem Privatunternehmen nicht offenbart wird, da dies in der vorliegenden Konstellation nicht erforderlich ist. Zwar werden die Daten beim Adressmittlungsverfahren nicht für den bei der Erhebung bestimmten Zweck genutzt, sondern mithilfe der Adressdaten Fragebögen eines Dritten direkt an den Betroffenen versandt, wobei die Betroffenen darüber entscheiden können, ob sie die gewünschten Angaben gegenüber dem Dritten machen wollen. Da jedoch keine Übermittlung an Dritte, sondern an den Betroffenen selbst stattfindet, die Daten verarbeitende Behörde also die Daten nur in einem minimalen Umfang nutzt, ist dieses Verfahren als zulässig anzusehen. Das öffentliche Interesse an dem geänderten Nutzungszweck muss allerdings die Interessen der Betroffenen, etwa an dem Wunsch, nicht durch unnötige Postsendungen belästigt zu werden, überwiegen. Gründe dafür könnten in der leichten Zugänglichkeit der Daten, der minimalen Intensität der informationellen Beeinträchtigung und der Möglichkeit, nicht an der Befragung teilzunehmen, gegeben sein (8. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Brandenburg, 11.2). Vorteil des allgemein als zulässig angesehenen Adressmittlungsverfahrens ist, dass vermieden wird, Adressen der Betroffenen Dritten zur Kenntnis gelangen zu lassen. Wenn das Verfahren so gestaltet ist, dass die Daten nur von den Mitarbeitern der Abfallwirtschaft bearbeitet und genutzt werden, ist das Verfahren der Adressmittlung als zulässig anzusehen.

Dass die angemessene Höhe der Kosten der Unterkunft auch ohne die Mitwirkung von privaten Unternehmen bestimmt werden kann, zeigt die Erfahrung anderer Thüringer Landkreise und kreisfreier Städte. In diesen Fällen orientieren sich die Sozialbehörden am Mietspiegel der jeweiligen Gebietskörperschaft. Hilfsweise nutzen sie auch Mietspiegel der regionalen Immobilienwirtschaft bzw. Angaben der kommunalen Wohnungsunternehmen, ohne dass dabei personenbezogene Daten übermittelt werden müssen.

Eine Mietwerterhebung zur Bestimmung einer angemessenen Höhe der Kosten der Unterkunft gemäß § 22 SGB II unter Nutzung regional verfügbarer Mietspiegel ohne Übermittlung personenbezogener Daten stellt die optimale datenschutzrechtliche Verfahrensgestaltung dar. Unter engen Voraussetzungen ist eine solche Mietwerterhebung auch unter Mitwirkung eines privaten Unternehmens durch Nutzung von Kundenadressen des kommunalen Abfallwirtschaftsbetriebs im Wege der Adressmittlung als zulässig anzusehen. Hingegen stellt eine Verarbeitung der Adressdaten der Abfallbehörde zum Zweck der Mietwerterhebung durch einen privaten Dritten einen Verstoß gegen datenschutzrechtliche Bestimmungen dar.

5.5 Datenschutzrechtliche Kontrolle von Frei- und Hallenbädern

Aufgrund einer Beschwerde hat der TLfD im Jahre 2010 eine landesweite Umfrage zur Videoüberwachung in kommunalen Schwimmbädern durchgeführt und insgesamt elf Bäder kontrolliert. In zehn Fällen wurden teilweise erhebliche Verstöße gegen den Datenschutz – bis hin zu Aufnahmen in einer Sauna – festgestellt. Kommunale Schwimmbäder sind öffentliche Stellen nach § 2 Abs. 1 ThürDSG und unterliegen damit der Kontrolle des TLfD. Da sie allerdings am Wettbewerb teilnehmen, gilt für sie das BDSG. Die Voraussetzungen für die Videoüberwachung sind in § 6 b BDSG geregelt. Schwimm- und auch Freibäder sind öffentlich zugänglich Räume im Sinne des Gesetzes. Damit kann die Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke zulässig sein. In beiden Fällen dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen. Unzulässig ist jede Beobachtung, die die Intimsphäre Betroffener berührt, weswegen eine Videoüberwachung,

die eine Beobachtung von Personen in Sanitarräumen, Umkleidekabinen und in der Sauna ermöglicht, generell zu unterlassen ist.

Das Hausrecht erlaubt es, nicht zahlenden Gästen oder sonstigen Störern den Zutritt zu verweigern oder sie aus der Einrichtung zu verweisen. Hierzu ist die Videoüberwachung insoweit nicht erforderlich, da der unberechtigte Zutritt in aller Regel durch andere Maßnahmen, wie hohe Drehkreuze oder Schranken, verhindert werden kann. Das Hausrecht berechtigt auch, Personen von Rechtsverstößen abzuhalten. Voraussetzung für den Einsatz von Videokameras in diesem Zusammenhang ist jedoch, dass es konkrete Anhaltspunkte wie Sachbeschädigung oder Diebstahl bereits gab und die Überwachung nicht anders gewährleistet werden kann, bspw., weil es sich um schwer einsehbare Räume handelt. Die Aufzeichnung ist aber auf das erforderliche Maß zu beschränken. Der Aufnahmebereich der Kamera ist direkt auf den betroffenen Bereich (Garderobenschränke, Kassenautomaten in Parkhäusern, Parkhausausfahrten u. ä.) zu richten. Unzulässig ist eine Aufzeichnung zum Schutz vor bloßen Bagatellschäden.

Bei der Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke ist danach zu differenzieren, ob die erzeugten Bilder gespeichert werden oder lediglich der Beobachtung dienen. Im letzteren Fall, dem sogenannten Monitoring, stellt der Monitor nur ein „verlängertes Auge“ des Betrachters dar. Diese Form der Videoüberwachung greift weniger intensiv in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen ein als eine Speicherung der Bilder. Eine aufzeichnunglose Überwachung kann zur Unterstützung der Aufsichtspflicht an gefährlichen, uneinsehbaren Stellen – wie bspw. Sprungtürmen und Rutschen – erforderlich sein. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, bspw. weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit sprechen. Nicht ausreichend ist wegen der nach § 6 b Abs. 1, letzter Halbsatz BDSG vorzunehmenden Abwägung mit den schutzwürdigen Interessen der Betroffenen die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Unzulässig ist auch eine Bildaufzeichnung zum rein vorsorglichen Ausschluss einer möglichen Beweisnot in künftigen Haftungsfällen. Es ist nicht verhältnismäßig, einen derartigen Grundrechtseingriff für eine Vielzahl von Personen hinzunehmen, nur um ein Haftungsrisiko des

Betreibers zu minimieren, da auch die Rechtsprechung keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen fordert.

§ 6 b Abs. 2 bis 5 BDSG enthält weitere Anforderungen an eine zulässige Videoüberwachung. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Der Betroffene muss erkennen können, an welchen Stellen das Schwimmbad videoüberwacht ist. Dies soll mit Hinweistafeln an den betroffenen Stellen erfolgen. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Eine Speicherdauer von zwei Wochen darf grundsätzlich nicht überschritten werden. Erfahrungsgemäß reicht dieser Zeitraum, um Beweismittel, etwa zu Sachbeschädigungen, zu sichern.

Anhand dieser Grundsätze wurden in Thüringen elf Schwimmbäder (Thüringentherme Mühlhausen, Schwimmbad Ichttershausen, Freizeitbad GalaxSea, Freibad Eisenberg, Ardesia Therme Bad Lobenstein, Erfurter Roland-Matthes-Schwimmbad, Ottilienbad Suhl, Freizeitzentrum „Rohrer Stirn“ Meiningen, Badehaus Nordhausen, Volksschwimmbad Sömmerda sowie Kur- und Familienbad "Tabbs" in Tabarz) geprüft. Zwei Bäder haben auf eine Speicherung der Videoaufnahmen verzichtet und die Kamera lediglich als verlängertes Auge eingesetzt. In den anderen Fällen wurde gefordert, einzelne Überwachungen einzustellen oder diese zeitlich und räumlich zu begrenzen und in der Nähe der jeweiligen Kameras auf die Videoüberwachung hinzuweisen. Bisher sind die Betreiber von drei Schwimmbädern den Forderungen des TLfD nachgekommen, sodass diese Kontrollen abgeschlossen werden konnten, wobei in einem Fall vollständig auf den Einsatz von Videokameras verzichtet wurde. In einem weiteren Bad ist mit einer baldigen Umsetzung der Forderungen zu rechnen. Noch unerledigt sind somit acht Kontrollen. Davon betreffen drei Fälle Schwimmbadbetreiber, die auf Anraten der Deutsche Bädergesellschaft entgegen der obigen Grundsätze die Auffassung vertreten, dass ein berechtigtes Interesse für eine Speicherung von Videoaufnahmen von schwer einsehbaren Bereichen, wie bspw. die Aus- und Eingänge von Rutschen, anzunehmen sei. Nur so sei es möglich, Beweismittel zur Abwehr von Schadenersatz-

ansprüchen vorzulegen. Schriftliche Stellungnahmen von zwei Betreibern stehen derzeit noch aus.

Im Falle der Thüringentherme Mühlhausen wurde eine Beanstandung gemäß § 39 ThürDSG ausgesprochen, da sich die zuständige Wirtschaftsbetriebe Mühlhausen GmbH geweigert hatte, einem festgestellten datenschutzrechtlichen Verstoß abzuweichen. In Ichtershausen beschloss der Gemeinderat, dem im Schwimmbad festgestellten Verstoß gegen datenschutzrechtliche Vorschriften nicht abzuweichen. Daher hat der TLfD eine Beanstandung gemäß § 39 ThürDSG ausgesprochen und die Kommunalaufsicht des zuständigen Landratsamtes gebeten, zur Herstellung eines ordnungsgemäßen datenschutzrechtlichen Zustandes beizutragen. Bei drei weiteren unerledigten Kontrollen sind von den Betreibern noch konkrete Sachverhalte nachzuweisen, die eine Videoüberwachung rechtfertigen.

Eine verdachtsunabhängige Videoüberwachung, insbesondere, wenn die Aufnahmen gespeichert werden sollen, stellt einen nicht unerheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Daher sind die rechtlichen Voraussetzungen sorgfältig vorab zu prüfen. Das Ergebnis dieser Prüfung ist nachvollziehbar zu dokumentieren. Auf die Überwachungsmaßnahmen ist erkennbar in der Nähe der Kameras hinzuweisen. Liegen die Voraussetzungen für eine Videoüberwachung nicht mehr vor, ist die Überwachung einzustellen.

5.6 Löschfristen

Immer wieder erreichen den TLfD Anfragen zu Speicher- und Löschfristen. So lag einer Beschwerde folgender Sachverhalt zugrunde: Nach Ablehnung seines Wohngeldantrags bat der Antragsteller die zuständige Wohngeldstelle bei der Stadt Ilmenau, die personenbezogenen Daten seines abgelehnten Wohngeldantrags zu löschen, da sie nicht mehr erforderlich seien. Hierauf wurde dem Antragsteller mitgeteilt, dass die Aufbewahrungsfrist für Wohngeldakten nach dem zu diesem Zeitpunkt geltenden Erlass des TIM vom 28. Mai 2002 sechs Jahre betrage, wobei diese Frist bei einer Versagung des Wohngeldes am 1. Januar des auf die Bescheiderteilung folgenden Kalenderjahres beginne. Daher dürfe die erbetene Daten-

löschung erst ab dem 1. Juli 2017 erfolgen. Bei einer Nachfrage durch den TLfD stellte sich heraus, dass die Fachaufsicht für das Wohngeldverfahren inzwischen vom TIM auf das TMBLV übergegangen war. Wie das TMBLV in seiner Stellungnahme mitteilte, solle ein novellierter Erlass zum Wohngeldverfahren ab dem 1. Januar 2011 in Kraft treten. Nach der Neuregelung endet bei abgelehnten bzw. versagten Erstanträgen die Aufbewahrungsfrist bereits am 31. Dezember des auf die Bescheiderteilung folgenden Kalenderjahres. Begründet wird diese Regelung damit, dass die Wohngeldstatistiken des TLS für das zurückliegende Kalenderjahr verfahrensbedingt bereits gegen Ende des Folgejahres durch das TLRZ erstellt werden. Es konnte Einigung mit der Wohngeldstelle erzielt werden, im Falle des Beschwerdeführers, mit Billigung des TMBLV, bereits vor Inkrafttreten des Erlasses im Sinne der Neuregelung zu verfahren. Im Ergebnis wurde die Wohngeldakte des Beschwerdeführers zum 31. Dezember 2011 vernichtet.

In einem anderen Fall bat die Stadtverwaltung Erfurt zu prüfen, welche Speicher- bzw. Löschfristen für Einkommensnachweise sowohl beim öffentlichem Träger (Jugendamt) als auch bei freien Trägern für notwendig erachtet werden. Das Rechnungsprüfungsamt der Stadt war der Ansicht, dass diese Belege zehn Jahre aufzubewahren sind. Die Aufbewahrungsfristen für (zahlungs-)begründende Unterlagen wie die Einkommensnachweise von Eltern zur Berechnung von Kita-Gebühren sind spezialgesetzlich in § 82 Thüringer Gemeindehaushaltsverordnung (ThürGemHV) geregelt, wonach die Belege nach § 82 Abs. 2 ThürGemHV sechs Jahre aufzubewahren sind. Nach § 82 Abs. 2 Satz 4 ThürGemHV sind Belege nur dann zehn Jahre aufzubewahren, wenn sich Zahlungsgrund und Zahlungspflichtige nicht aus den Büchern ergeben. Die beim Jugendamt geführten Vorbücher zum Sachbuch sind als Bücher in diesem Sinne anzusehen, zumal sie beim Jugendamt zehn Jahre aufzubewahren sind. Da die in den Vorbüchern aufgeführten Personenkonto-Aufschlüsse über die jeweiligen zahlungspflichtigen Eltern ermöglichen und damit das Vorbuch zusammen mit dem Sachbuch alle notwendigen Angaben (Zahlungsgrund und Zahlungspflichtiger) enthalten, trifft die Voraussetzung des § 82 Abs. 2 Satz 4 ThürGemHV für eine zehnjährige Aufbewahrung der Belege nicht zu und es ist nur eine Aufbewahrungsfrist von sechs Jahren für die Einkommensnachweise zur Berechnung der Kita-Gebühren zum Zwecke der Rechnungsprüfung zulässig. In diesem Zusammenhang wurde mitgeteilt, dass alle

nicht dem Nachweis des Einkommens der Betroffenen dienenden personenbezogenen Daten, wie bspw. die Religionszugehörigkeit, geschwärzt werden dürfen, nicht jedoch die zur Gebührenberechnung erforderlichen Daten.

Bei abgelehnten bzw. versagten Erstanträgen auf Wohngeld ist die Aufbewahrungsfrist wesentlich verkürzt worden. Damit wurde dem datenschutzrechtlichen Erforderlichkeitsprinzip Rechnung getragen. Eine Aufbewahrungsfrist von sechs Jahren für die Einkommensnachweise zur Berechnung von Kita-Gebühren zum Zwecke der Rechnungsprüfung ist zulässig. Alle nicht dem Nachweis ihres Einkommens dienenden personenbezogenen Daten dürfen von den Betroffenen geschwärzt werden.

5.7 Zeiterfassung im Kindergarten

Aufgrund einer Beschwerde wurde bekannt, dass die Kinder eines kommunalen Kindergartens bzw. deren Eltern mit Zeiterfassungschips ausgestattet wurden, um festzustellen, wann sie jeweils in den Kindergarten gebracht und abgeholt werden. Wie die Verwaltungsgemeinschaft Apfelstädt auf Nachfrage des TLfD mitteilte, diene die Erfassung der Anwesenheitszeiten der Kinder mittels des chipgestützten Zeiterfassungssystems der Erhebung von Elternbeiträgen und beruhe auf der Benutzung- sowie der Beitragsatzung des Kindergartens der Gemeinde. Um die Wahl zwischen drei Betreuungszeiten bei der Berechnung der Elternbeiträge nachvollziehen zu können, seien die Anwesenheitsdaten der Kinder genau zu erfassen. Das Zeiterfassungssystem entlaste die Erzieherinnen, die ansonsten die Daten der Anwesenheit notieren müssten. Hierfür seien die beteiligten Eltern zur Abgabe einer schriftlichen Einverständniserklärung aufgefordert worden. Die erfassten Daten dürften nur für die Abrechnung der Elternbeiträge genutzt werden. Der PC zum Abruf der Daten stehe im Büro der Kindergartenleiterin und sei mittels einer verschließbaren Kappe gegen unberechtigte Zugriffe gesichert. Die Elternbeiträge seien einmal pro Monat durch die Leiterin des Hauptamtes im Kindergarten anhand der programmtechnischen Auflistung festzulegen. Dies entlaste die Kindergartenleiterin. Nach § 4 Abs. 1 ThürDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betrof-

fene eingewilligt hat. In diesem Zusammenhang sind auch Satzungen als Rechtsvorschriften anzusehen. Nach § 19 ThürDSG ist das Erheben der personenbezogenen Daten zulässig, wenn ihre Kenntnis für die Aufgaben der erhebenden Stelle erforderlich ist. Da die erhobenen Aufbewahrungsdaten der Gebührenfestlegung dienen, liegt eine zulässige Datenerhebung vor; einer Einwilligung hätte es nicht bedurft.

Weil es sich bei dem Zeiterfassungs- und Auswertungssystem um ein automatisiertes Verfahren zur Verarbeitung personenbezogener Daten nach § 3 Abs. 2 ThürDSG handelt, wurde die Gemeinde gebeten, folgenden datenschutzrechtlichen Dokumentations- und Regelungsverpflichtungen nachzukommen, die u. a. der Herstellung der notwendigen Transparenz des Verfahrens dienen:

1. Verfahrensverzeichnis gemäß § 10 ThürDSG: Das Verfahren ist in dem Verzeichnis automatisierter Verfahren des Kindergartens – unter Verwendung der Formblätter entsprechend den Hinweisen des TIM zum ThürDSG zu dokumentieren.
2. Schriftliche Freigabe gemäß § 34 Abs. 2 ThürDSG: Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf einer datenschutzrechtlichen Freigabe.
3. Technische und organisatorischen Maßnahmen gemäß § 9 ThürDSG: Zur Gestaltung eines solchen automatisierten Verfahrens ist insbesondere seine technische Gestaltung, die Maßnahmen zur Gewährleistung der Vertraulichkeit (Abdeckung, Passwortschutz, zugriffsberechtigte Personen und Regelung zur monatlichen Gebührenberechnung) in geeigneter Weise Form einer Dienstanweisung zu fixieren.

Wie die Verwaltungsgemeinschaft mitteilte, seien die Forderungen des TLfD inzwischen umgesetzt worden.

Nach § 4 Abs. 1 ThürDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. In diesem Sinne sind auch Satzungen als Rechtsvorschriften anzusehen.

Jedes automatisierte Verfahren zur Verarbeitung personenbezogener Daten unterliegt den Dokumentations- und Regelungsverpflichtungen des ThürDSG.

5.8 Firmenumsatz und Fremdenverkehrsabgabe - Fortsetzung

Bereits im 8. Tätigkeitsbericht (5.7) des TLfD wurde über diese Beschwerde berichtet. Dabei hatte der TLfD die Unzulässigkeit der an einen Unternehmer gerichteten Forderung der Verwaltungsgemeinschaft Rennsteig, den Jahresumsatz seines Produktionsunternehmens zur Berechnung der Fremdenverkehrsabgabe anzugeben, festgestellt. Daraufhin erklärte sich die Verwaltungsgemeinschaft zunächst bereit, die von ihr als Rechtsgrundlage der o. g. Auskunftspflicht genannte Fremdenverkehrsbeitragssatzung derart zu ändern, dass künftig die Veranlagung der ortsansässigen Gewerbetreibenden eindeutig und datenschutzkonform geregelt wird. Nachfolgend wurde der Beschwerdeführer jedoch von der Verwaltungsgemeinschaft Rennsteig erneut zur Abgabe einer Erklärung zur Veranlagung des Fremdenverkehrsbeitrags aufgefordert, obwohl der Verwaltungsgemeinschaft die datenschutzrechtliche Beurteilung der Angelegenheit bekannt war. Daraufhin hat der TLfD die Verwaltungsgemeinschaft Rennsteig aufgrund der im Wiederholungsfall verlangten unzulässigen Datenerhebung gemäß § 39 ThürDSG beanstandet und gefordert, einen datenschutzrechtskonformen Zustand herzustellen. Dessen ungeachtet wurde der Beschwerdeführer nochmals aufgrund der unveränderten Fremdenverkehrsbeitragssatzung datenschutzwidrig zur Vorlage des Umsatzes aufgefordert, woraufhin der TLfD das TLVwA gebeten hatte, hiergegen aufsichtsrechtlich vorzugehen. Das TLVwA teilte zwar die Wertung des TLfD, teilte jedoch – wie bereits zuvor die Kommunalaufsicht des Landratsamtes Ilm-Kreis – mit, dass keine kommunalaufsichtlichen Maßnahmen zu veranlassen seien, da dem Betroffenen grundsätzlich der Rechtsweg nach Artikel 19 GG offen stehe.

Diese Rechtsansicht wird vom TLfD nicht geteilt. Aufsichtsrechtliche Mittel stehen nicht unter dem Vorbehalt einer Erschöpfung des Rechtsweges durch den Betroffenen. Gleichwohl teilte der TLfD dem Beschwerdeführer mit, dass die Fortführung seines Beschwerdeorgans derzeit nicht Erfolg versprechend sei, da dem TLfD keine aufsichtsrechtlichen Befugnisse gegenüber den Kommunalbe-

hörden zu Gebote stehen. Ob der TLfD gegenüber den Aufsichtsbehörden weitere Maßnahmen ergreifen wird, ist derzeit Gegenstand einer Prüfung.

In Einzelfällen sieht sich der TLfD derzeit mangels aufsichtsrechtlicher Befugnisse gegenüber den Kommunalbehörden außerstande, berechtigten Beschwerden gemäß § 11 ThürDSG abzuwehren, obwohl selbst die zuständige Aufsichtsbehörde einen Verstoß gegen Datenschutzrecht einräumt. Dies spricht dafür, dass die gesetzlichen Eingriffsrechte des TLfD ausgeweitet werden müssen, um einen wirksamen Datenschutz für alle Bürger auch tatsächlich durchsetzen zu können.

Künftige Änderungen im EU-Datenschutzrecht lassen erwarten, dass die Datenschutzbehörden auch Aufsichtsfunktionen gegenüber öffentlichen Stellen wahrnehmen sollen.

5.9 Bundesmeldegesetz/Fortentwicklung des Meldewesens

Das Meldewesen wurde mit der Föderalismusreform I im Herbst 2006 in die ausschließliche Gesetzgebungskompetenz des Bundes überführt (Artikel 73 GG). Das Gesetz zur Fortentwicklung des Meldewesens soll dabei das geltende Melderechtsrahmengesetz sowie die bisherigen Landesmeldegesetze ersetzen. Der TLfD hatte dem TIM bereits 2008 einen umfassenden Katalog an datenschutzrechtlichen Forderungen zum damaligen Referentenentwurf zur Verfügung gestellt und sich auch 2011 am aktualisierten Entwurf mit einer Stellungnahme beteiligt. Obwohl eine Anzahl der im Kreise der Datenschutzbeauftragten des Bundes und der Länder abgestimmten Datenschutzforderungen in den Entwurf übernommen wurde, hatte der TLfD insbesondere gefordert, im Zuge der Modernisierung des Melderechts die bisherigen Widerspruchsregelungen auf den Prüfstand zu stellen und im Interesse des Bürgers durch Einwilligungslösungen zu ersetzen. Künftig sollen bei einfachen Melderegisterauskünften zu gewerblichen Zwecken diese Auskünfte nur noch zweckgebunden erteilt werden und für Auskünfte zu Zwecken des Adresshandels und der Werbung eine Einwilligung der betroffenen Person in die Übermittlung für jeweils diesen Zweck erforderlich sein. Der Weitergabe seiner Daten an Parteien, Wählergruppen und andere

Träger von Wahlvorschlägen im Zusammenhang mit Wahlen, an Mandatsträger, Presse oder Rundfunk hinsichtlich Alters- oder Ehejubiläen sowie an Adressbuchverlage muss der Betroffene aber weiterhin widersprechen, wenn er die genannte Übermittlung seiner Daten nicht wünscht. Der Deutsche Bundestag hatte zum Redaktionsschluss noch nicht über den Gesetzentwurf entschieden.

Wenn der Gesetzentwurf unverändert beschlossen wird, ist auch zukünftig von einer Vielzahl von Anfragen und Beschwerden von Bürgern auszugehen, deren Daten in Adressbüchern veröffentlicht, von Parteien zu Zwecken der Wahlwerbung oder durch die Medien bei Alters- und Ehejubiläen genutzt werden.

5.10 Zweckentfremdung der Hotelmeldedaten

Im Berichtszeitraum wurde der TLfD darüber informiert, dass in der Kurstadt Brotterode der zum Einsatz kommende Meldeschein für Beherbergungsstätten auch dazu genutzt wurde, neben den für die Erfüllung der melderechtlichen Bestimmungen und für die Berechnung der Kurabgabe erforderlichen Daten noch zusätzlich personenbezogene Daten für statistische Auswertungen zu erheben. Gemäß § 24 Abs. 2 ThürMeldeG haben Personen, die in einer Beherbergungsstätte aufgenommen werden, am Tag ihrer Ankunft einen besonderen Meldeschein auszufüllen. Darüber hinaus dürfen von Gemeinden nach § 25 Abs. 3 ThürMeldeG für Zwecke der Erhebung des Kurbeitrags nach § 9 ThürKAG sowie für die Fremdenverkehrs- und Beherbergungsstatistik erforderliche Angaben erhoben und verarbeitet und Durchschriften der besonderen Meldescheine gefertigt werden. In diesem Fall ist der Meldepflichtige im Meldeschein darauf hinzuweisen. Nach § 26 Abs. 1 ThürMeldeVO ist als Meldeschein für Beherbergungsstätten nach § 25 Abs. 1 und 2 ThürMeldeG der Vordruck nach dem Muster der Anlage 9 zu verwenden. Gemeinden, in denen ein Kurbeitrag erhoben wird, können nach Maßgabe des § 25 Abs. 3 ThürMeldeG Vordrucke nach den Mustern der Anlagen 10, 10a und 10b nutzen (§ 26 Abs. 2 ThürMeldeVO). Diese Vordrucke erfüllen die datenschutzrechtlichen Grundsätze dahingehend, dass mit ihnen nur solche Daten erhoben und insbesondere auch an die jeweilige Kommune übermittelt werden, die zu ihrer Aufgabenerfüllung (Abrechnung der Kurbeiträge) erforderlich sind. Da die Vordrucke zur

Vereinfachung im Durchschreibeverfahren gestaltet sind, werden in den Durchdrucken die für die Ausstellung der Gästekarte und die Abführung des Kurbeitrages nicht notwendigen Angaben jeweils geschwärzt. Die Gemeinde, in der Kurbeiträge erhoben werden, kann entscheiden, ob bei ihr unter Verwendung der Muster (Anlagen 10, 10 a und 10 b zur ThürMeldeVO) mit dem Meldeschein auch die Kurbeiträge abgerechnet werden sollen oder alternativ Anlage 9 zur ThürMeldeVO als Meldeschein verwendet und zur Erhebung des Kurbeitrags ein gesondertes Verfahren genutzt wird. Im letztgenannten Fall ist aber gleichfalls zu sichern, dass die konkrete Datenverarbeitung in einer Satzung geregelt und auf das erforderliche Maß beschränkt wird.

Diese für alle Kommunen durch Rechtsvorschrift verbindlich geregelte Verfahrensweise wurde von der Stadt Brotterode nicht eingehalten. Weder die verwendeten Meldescheine, die in der Satzung enthaltenen Formulierungen noch die getroffenen Festlegungen entsprachen den gesetzlichen Vorgaben des ThürMeldeG und der ThürMeldeVO. Darüber hinaus wurden mit den Meldescheinen statistische Daten ohne Rechtsgrundlage erhoben, da es hierzu nach dem ThürStatG selbst bei freiwilligen Auskünften neben einer entsprechenden Satzung auch der Einrichtung einer Statistikstelle bedurft hätte (§§ 22, 23 ThürStatG). Im Hinblick auf diese Verstöße gegen die Bestimmungen zum Datenschutz hat der TLfD gefordert, das Verfahren und die Satzung kurzfristig den geltenden Rechtsvorschriften anzupassen und bis zur Neuregelung auf die Verarbeitung der unzulässig erhobenen Daten zu verzichten. Seitens der Kurstadt wurde entsprechend den Hinweisen des TLfD eine Änderung der Kurbeitragssatzung vorgenommen. Zudem hat die Stadt auch den Meldeschein für die Beherbergungsstätten so verändert, dass die freiwilligen statistischen Angaben entfallen sind. Damit entsprechen nunmehr sowohl die Satzung als auch der verwendete Meldeschein den datenschutzrechtlichen Vorgaben.

Grundsätzlich ist mittels der Meldescheine für Beherbergungsstätten auch die Erhebung statistischer Daten rechtskonform möglich, wenn die Freiwilligkeit der Auskunft aus dem Meldeschein eindeutig hervorgeht. Dann bedarf es aber nach dem ThürStatG auch bei freiwilligen Auskünften neben einer entsprechenden Satzung der Einrichtung einer Statistikstelle.

5.11 Zugriffsprotokollierung und Auswertung im Meldeamt

Ein Bürger erhielt auch nach einem Wohnungswechsel innerhalb der Stadt Erfurt anonyme Briefe mit nach seinem Verständnis für ihn ehrverletzendem Inhalt. Er ging davon aus, dass seine neue Adresse lediglich fünf Personen bekannt sei, die für ihn als anonyme Briefeschreiber aber nicht in Frage kämen und vermutete eine „missbräuchliche Verwendung“ seiner personenbezogenen Daten im Meldeamt, sodass er sich hilfeschend an den TLfD wandte.

Gemäß § 31 Abs. 1 ThürMeldeG darf die Meldebehörde aus dem Melderegister jedermann Auskunft über die Anschrift eines konkret bestimmten Einwohners erteilen. Diese Melderegisterauskunft ist gemäß § 31 Abs. 7 ThürMeldeG bei Vorliegen einer Auskunftssperre im Melderegister unzulässig. Auskunftssperren können bei der Meldebehörde im Einzelfall auf Antrag des Betroffenen eingerichtet werden. Voraussetzung dafür ist, dass dieser der Meldebehörde das Vorliegen von Tatsachen glaubhaft macht, die die Annahme rechtfertigen, dass ihm oder einer anderen Person bei einer Auskunftserteilung eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder schutzwürdige Belange erwachsen kann. Zudem ist eine einfache Melderegisterauskunft (Vor- und Familienname, Anschrift) auch durch automatisierten Abruf über das Internet (§ 31 Abs. 3 ThürMeldeG) möglich, soweit der Betroffene keinen Widerspruch gegen diese Form der Auskunftserteilung bei der für ihn zuständigen Meldebehörde eingelegt hat.

Unabhängig von dieser sogenannten „Jedermannsauskunft“, für den Beschwerdeführer war nach seinen Angaben keine Auskunftssperre gemäß § 31 Abs. 7 ThürMeldeG und auch kein Widerspruch gemäß § 31 Abs. 3 ThürMeldeG im Melderegister eingetragen, hat der TLfD diese Beschwerde zum Anlass genommen, das zuständige Meldeamt hinsichtlich des Verfahrens bei Melderegisteranfragen (einschließlich der technischen und organisatorischen Regelungen zur Protokollierung und Auswertung der Protokolldaten im Verfahren bei Datenabfragen) zu kontrollieren.

Vor Ort wurde festgestellt, dass das Verfahren ein verfahrensinternes Protokollierungswerkzeug beinhaltet, mit dem nach Angaben der Ansprechpartner sämtliche lesenden und schreibenden Zugriffe auf die Meldedaten (Benutzerkennung, Datum und Uhrzeit des Zugriffs, Anzahl der Treffer für die Suchanfrage, die verwendeten Suchkrite-

rien sowie als Zusatzinformationen der Name, der Rufname und das Geburtsdatum zum aufgerufenen Datensatz) durch Mitarbeiter des Meldeamtes protokolliert werden. Die Protokolldaten sind dabei nicht gesondert abgelegt, sondern im Verfahren selbst gespeichert und werden vom Systemadministrator jeweils für das vorvergangene Quartal alle drei Monate gelöscht. Die Prüfung der Protokolldaten erfolgt nach der im Meldeamt geltenden Dienstvereinbarung nur bei Verdacht auf Missbrauch bzw. Verstoß gegen die Regelungen der Dienstvereinbarung mit vorheriger Zustimmung des Personalrats. Auf Veranlassung des TLfD erfolgte eine Auswertung der Zugriffe auf den Datensatz des Beschwerdeführers für den in Rede stehenden Zeitraum (auf den Umzug des Beschwerdeführers folgender Tag bis zum Kontrolltermin). Diese ergab mehrere Zugriffe in dieser Zeit durch insgesamt sechs Mitarbeiter des Meldeamtes.

Die Protokollierung der in Abhängigkeit von der Zuständigkeit lesenden oder schreibenden Zugriffe auf die Meldedaten durch die Mitarbeiter im Meldeamt wurde vom TLfD als Maßnahme der Datensicherheit nach § 9 Abs. 2 Nr. 5 ThürDSG (Revisionsfähigkeit) und § 7 Abs. 4 Satz 4 i. V. m. Absatz 6 ThürDSG (Abrufverfahren innerhalb einer Daten verarbeitenden Stelle) als geboten bewertet. Die vorgelegte Dienstvereinbarung enthielt aber nur die notwendigsten Regelungen zur Zulässigkeit und Beteiligung des Personalrats, sodass der TLfD empfohlen hat, die notwendigen Maßnahmen und das konkrete Verfahren bei einer Missbrauchskontrolle durch die Dienststelle und den Personalrat näher festzulegen. Da es sich bei den Protokolldaten ebenfalls um personenbezogene Daten der Mitarbeiter und der Bürger (Name und Geburtsdatum werden mitprotokolliert) handelt, hat der TLfD darauf hingewiesen, dass es auch beim Zugriff auf die Protokolldaten mit einem Auswertewerkzeug nach § 9 Abs. 2 ThürDSG organisatorischer Maßnahmen bedarf, die einen unbefugten Zugriff ausschließen oder zumindest befugte Zugriffe nachvollziehbar machen. So sind entweder technische Maßnahmen zu ergreifen, die einen Zugriff auf die Protokolldaten nur im Vier-Augen-Prinzip ermöglichen oder es müssen zumindest die Auswertungen der Protokolldaten ebenfalls protokolliert werden (siehe Orientierungshilfe des AK „Technische und organisatorische Datenschutzfragen“ der DSK zur Protokollierung, www.thueringen.de/imperia/md/content/datenschutz/orientierungshilfe/protokollierung.pdf).

Dem Beschwerdeführer hat der TLfD im Ergebnis mitgeteilt, dass zwar Zugriffe durch Mitarbeiter der Meldebehörde auf seinen Meldedatensatz im fraglichen Zeitraum erfolgten, diese aber nach Mitteilung des Meldeamtes zur Erfüllung der diesen Mitarbeitern zugewiesenen Aufgaben – dazu gehört u. a. auch die Erteilung von Melderegisterauskünften – erfolgt sind. Die datenschutzrechtliche Zulässigkeit der Zugriffe der Mitarbeiter der Meldebehörde auf seinen Datensatz im Melderegister hat der TLfD deshalb als gegeben angesehen. Auch nach dem Wohnungswechsel des Beschwerdeführers war es einer Vielzahl von Personen möglich, sich mittels einfacher Melderegisterauskunft gemäß § 31 Abs. 1 ThürMeldeG sowie gemäß § 31 Abs. 3 ThürMeldeG hinsichtlich der (neuen) Anschrift zu informieren. Um zumindest die o. g. Melderegisterauskunft mittels automatisierten Abrufs über das Internet zu unterbinden, hat der TLfD dem Beschwerdeführer empfohlen, formlos oder mittels Formblatt (http://www.thueringen.de/imperia/md/content/datenschutz/veroeffentlichungen/mustervordrucke/widerspruch_gegen_melddatenuebermittlung.pdf) bei der zuständigen Meldebehörde Widerspruch gegen derartige Datenübermittlungen einzulegen.

Liegt keine Auskunftssperre des Betroffenen im Melderegister vor, ist eine datenschutzrechtliche Zulässigkeit der Übermittlung der nach einem Wohnsitzwechsel neuen Anschrift des Betroffenen an jedermann gemäß § 31 Abs. 1 ThürMeldeG grundsätzlich gegeben. Sofern es sich bei Protokolldaten um personenbezogene Daten handelt, sind durch die öffentlichen Stellen die technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG zur Gewährleistung des Datenschutzes zu treffen.

5.12 Zentrales Personenstandsregister

Das zum 1. Januar 2009 in Kraft getretene neue Personenstandsgesetz (PStG) beinhaltet neben einer umfassenden Überarbeitung des Personenstandsrechts die Einführung elektronischer Personenstandsregister in den Standesämtern. Zum 1. Januar 2014 ist die elektronische Registerführung in ganz Deutschland verpflichtend vorgeschrieben. Gemäß § 67 Abs. 1 PStG dürfen die Länder zentrale Register zu dem Zweck errichten, die Registerinträge der angeschlossenen Standesämter zu erfassen und den Standesämtern ihre Benutzung nach § 67 Abs. 3 PStG zu ermög-

lichen. § 67 Abs. 3 PStG ermöglicht dabei nicht nur dem den Registereintrag führenden Standesamt, sondern allen an das zentrale Personenstandsregister angeschlossenen Standesämtern die Benutzung der Personenstandsregister nach Maßgabe der §§ 55, 61 bis 66 PStG. Die Landesregierungen sind nach § 74 Abs. 1 Nr. 3 PStG ermächtigt, durch Rechtsverordnung ein zentrales elektronisches Personenstandsregister einzurichten und nähere Bestimmungen zu dessen Führung zu treffen. Dem TLfD war vom TIM zwar im Vorfeld der entsprechende Verordnungsentwurf zur Kenntnis gegeben worden, der konträren Rechtsauffassung des TLfD zum Verordnungsentwurf wurde aber nicht gefolgt. Nach Auffassung des TLfD stellt nämlich der § 74 Abs. 1 Nr. 3 i. V. m. § 67 PStG gerade keine ausreichende Ermächtigungsgrundlage für eine Verordnungsregelung zur Führung der jeweiligen elektronischen Personenstandsregister nach § 3 Abs. 2 PStG durch die Standesämter im zentralen Register dar, weil nach dem Wortlaut von § 67 PStG nur ein zentrales Register eingerichtet werden darf, an das die jeweiligen Standesämter ihre Daten übermitteln bzw. aus dem sie die Daten abrufen dürfen. Dabei gäbe es nur eine verantwortliche Stelle, nämlich diejenige, die das zentrale Register betreibt. Etwas anderes ist jedoch ein Verfahren, bei dem viele einzelne Stellen für den Inhalt einer zentralen (gemeinsamen) Datei verantwortlich sind und aus dieser Datei nicht nur Daten abrufen oder dorthin übermitteln, sondern den Datenbestand selbständig ändern dürfen. Hier handelt es sich um ein sogenanntes Verbundverfahren. Zum damaligen Zeitpunkt enthielt auch das ThürDSG keine entsprechende Regelung zu Verbundverfahren.

Allerdings ist zum 9. Dezember 2011 mit dem § 7 a ThürDSG (Gesetz zur Änderung des Thüringer Datenschutzgesetz und anderer Gesetze) eine Vorschrift in Kraft getreten, die nunmehr die Einrichtung derartiger Verfahren erlaubt, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

Der TLfD wird die Führung des zentralen Personenstandsregisters weiter kritisch begleiten.

5.13 Nutzung von Sterbebüchern in Archiven

An den TLfD hat sich ein Verein gewandt, der sich u. a. mit Recherchen und der Erstellung von Dokumentationen von Schicksalen der Gefallenen und Vermissten beider Weltkriege sowie der Opfer der sowjetischen Speziallager nach 1945 beschäftigt. Der Antrag des Vereins an das Stadtarchiv Köllda auf Einsicht bzw. Durchsicht der betreffenden Sterbebücher (bis einschließlich Sterbejahrgang 1978) war vom Bürgermeister der Stadt abschlägig beschieden worden.

Mit der Novellierung des PStG haben sich zum 1. Januar 2009 Änderungen hinsichtlich der Aufbewahrung und Fortführung der Personenstandsregister, die sich bisher stets in der Zuständigkeit der Standesämter befunden haben, ergeben. Gemäß § 5 Abs. 5 Nr. 3 PStG gilt für die Fortführung der Sterberegister eine Frist von 30 Jahren. Nach Ablauf dieser Frist sind nunmehr gemäß § 7 Abs. 3 PStG diese Register nach den jeweiligen archivrechtlichen Vorschriften den zuständigen öffentlichen Archiven zur Übernahme anzubieten. Mit der Übernahme der Unterlagen in ein öffentliches Archiv gelten in Thüringen für deren Nutzung jeweils Satzungen (Archivordnungen), die sich am ThürArchivG orientieren müssen. Danach hat gemäß § 16 ThürArchivG zunächst jedermann das Recht, Archivgut in öffentlichen Archiven nach Ablauf der Schutzfristen (§ 17 ThürArchivG) zu nutzen, der ein berechtigtes Interesse an der Benutzung insbesondere zu amtlichen, wissenschaftlichen, publizistischen oder Bildungszwecken glaubhaft macht. Hierzu zählen z. B. auch die Recherche zur Erkundung der Heimatgeschichte oder die Erstellung einer Chronik. Die Benutzung von Archivgut ist aber einzuschränken oder zu versagen, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange betroffener Personen oder Dritter (insbesondere Nachkommen oder sonstige Verwandte) beeinträchtigt werden (§ 18 ThürArchivG). Es ist deshalb Aufgabe des Archivs, generell vor der Benutzung von Archivgut diese datenschutzrechtlichen Aspekte zu prüfen.

Zur Klärung der Angelegenheit hatte der TLfD mit der Stadtverwaltung Kontakt aufgenommen und um Übersendung der Archivsatzung und Mitteilung der Ablehnungsgründe für die Einsicht in die Sterberegister des Archivs gebeten.

Dem TLfD wurde die geforderte Unterlage zur Verfügung gestellt und mitgeteilt, in den betreffenden Archivunterlagen würden sich auch personenbezogene Daten von anderen Personen wie Nachtragungen zu Sterbefällen und Daten zu Todesursachen der jeweiligen Personen befinden, sodass nach Ermessen der Stadtverwaltung dem Verein eine Einsichtnahme hinsichtlich der betreffenden Archivunterlagen verwehrt worden sei. Der TLfD hat darauf hingewiesen, dass eine Aushändigung von Kopien aus den Sterbebüchern mit Schwärzungen der entsprechenden schutzwürdigen Textpassagen an den Verein in Frage käme. Dazu hat die Stadtverwaltung ausgeführt, der Verein erhalte bereits seit geraumer Zeit Ablichtungen von Gefallenen aus den Personenstandsbüchern; nur leider könne dies aus verschiedenen Gründen nicht mit der vom Verein gewünschten Schnelligkeit erfolgen. Dem TLfD lagen die in Rede stehenden Sterbelisten nicht vor. Für das Einsichtsbegehren des Vereins bleibt aber ohne Bedeutung, ob der TLfD davon ausgeht, dass o. g. oder ähnliche datenschutzrechtliche Versagensgründe vorliegen. Aus dem ThürDSG lässt sich lediglich ein Anspruch auf „Auskunft über die zu seiner (der eigenen) Person gespeicherten Daten“ gemäß § 13 ThürDSG begründen; einen Anspruch auf Auskunft zu Daten dritter Personen (Recherche von Daten Dritter) beinhaltet jedenfalls das ThürDSG nicht. Die Durchsetzung eines möglichen Anspruchs auf Einsicht in die Sterbebücher kann demzufolge nicht durch den TLfD erfolgen.

Auch wenn keine datenschutzrechtlichen Versagensgründe für eine Einsicht in Archivunterlagen vorliegen, kann ein Anspruch darauf nicht aus dem ThürDSG abgeleitet werden.

5.14 Hundehalterregister mit Mängeln

Nach einer tödlichen Beißattacke eines gefährlichen Hundes im Mai 2010 hat die Landesregierung im Herbst 2010 den Entwurf eines Gesetzes zum Schutz der Bevölkerung vor gefährlichen Tieren (GefTierG) vorgelegt. Im Rahmen der parlamentarischen Beratungen wurde ohne Beteiligung des TLfD eine Verpflichtung aller Hundehalter aufgenommen, den Hund dauerhaft und unverwechselbar mit einem fälschungssicheren elektronisch lesbaren Transponder nach ISO-Standard (Mikrochip) durch einen Tierarzt kennzeichnen zu lassen. Es wird hier allgemein vom sogenannten „Chippen“ des

Hundes gesprochen. Zusätzlich wird der Halter verpflichtet, der zuständigen Behörde die Kennzeichnung anzuzeigen. Die Behörde darf dann die gespeicherten Daten im Rahmen der Erfüllung ihrer Aufgaben nach dem GefTierG zur Feststellung der Person des Halters nutzen. Schließlich wird das für das Ordnungsrecht zuständige Ministerium ermächtigt, die Art und Weise der Kennzeichnung und die Verwendung der personenbezogenen Daten des Hundehalters durch Rechtsverordnung zu regeln. Eine Regelung zur Einrichtung eines landesweiten Hundehalterregisters enthält das Gesetz jedoch nicht, obwohl in der abschließenden Parlamentsdebatte von einem Abgeordneten ausdrücklich darauf hingewiesen wurde, dass es dafür insoweit einen Bedarf gegeben hätte, als ein herrenloser Hund außerhalb des Zuständigkeitsbereichs aufgefunden wird. Genau ein solches Register beabsichtigte nach Inkrafttreten des Gesetzes nun das TIM mit der Chippflichtverordnung einzuführen und hat den Verordnungsentwurf dem TLfD zur Stellungnahme übersandt. Danach soll beim TLRZ ein zentrales Fachverfahren mit der Bezeichnung „Thüringer Hunderegister“ eingerichtet werden. Wenn dieses Register nur die Transponderdaten der „gechipten“ Hunde und einen Verweis auf die zuständige Ordnungsbehörde enthalten würde, wäre dagegen auch nichts einzuwenden. Allerdings sollen nach § 3 Abs. 2 des Verordnungsentwurfs auch die Namen und Anschriften aller Hundehalter in das Register aufgenommen werden, weshalb die Bezeichnung „Thüringer Hundehalterregister“ den Inhalt der Zentraldatei sehr viel genauer erfassen würde. Für ein solches Hundehalterregister fehlt es im Gesetz jedoch an einer hinreichend bestimmten Ermächtigungsgrundlage. Die Ermächtigung in § 2 Abs. 4 Satz 4 GefTierG zur Regelung der Verwendung der personenbezogenen Daten des Hundehalters kann nicht die Einrichtung eines landesweiten Registers rechtfertigen. Aus der Systematik des GefTierG ist nicht zu entnehmen, dass neben der Kennzeichnungs- und Anzeigepflicht in § 2 Abs. 4 ein zentrales Hunde(halter)register vorgesehen ist. So lässt sich aus dem Gesetz oder dessen Begründung nicht ermitteln, dass die Einrichtung eines Zentralregisters Bestandteil des durch den Gesetzgeber gesetzten Programms ist, das durch die Verordnung erreicht werden soll. Weitere verfassungsrechtliche Bedenken gegen die Einführung eines landesweiten Hundehalterregisters ergeben sich aus dem Rechtsstaatsprinzip (Artikel 20 GG/Artikel 44 ThürVerf) abgeleiteten Grundsatz des Vorbehalts des Gesetzes. Nach der Rechtsprechung

des Bundesverfassungsgerichts sind wesentliche Entscheidungen, insbesondere wenn diese wie hier in die Grundrechte der Bürger aus Artikel 2 Abs. 1 i. V. m. Artikel 1 GG bzw. Artikel 6 Abs. 1 ThürVerf eingreifen, dem parlamentarischen Gesetzgeber vorbehalten. Dies gilt jedenfalls für die grundlegenden Bestimmungen, sodass allenfalls Ausführungsbestimmungen dem Verordnungsgeber vorbehalten werden können. Dies zeigt auch die Regelungsstruktur in Sachsen-Anhalt und Hamburg, wo vergleichbare zentrale Register jeweils auf der Grundlage einer formalgesetzlichen Vorschrift eingerichtet wurden. Lediglich in Nordrhein-Westfalen ist ein Register auf der Grundlage einer Verordnung eingerichtet, allerdings enthält dieses im Unterschied zum vorgesehenen Register keine personenbezogenen Daten des Hundehalters. Schließlich war bei der vorgesehenen Regelung auch der Grundsatz der Verhältnismäßigkeit nicht gewahrt. Zwar ist eine zentrale Registrierung auch der Namen der Hundehalter geeignet, den dargestellten Zweck der raschen und zuverlässigen Ermittlung des Hundehalters zu ermöglichen. Allerdings fehlt es bei der zentralen Registrierung der Daten des Hundehalters an der Erforderlichkeit, weil weniger in die Grundrechte der Betroffenen eingreifende, jedoch gleich geeignete Regelungskonzepte zur Verfügung stehen. So ist die rasche und zuverlässige Ermittlung des Halters bei Aufgreifen eines Hundes in einem anderen Zuständigkeitsbereich auch dadurch möglich, dass in einem zentralen Register nur die Kennnummer des Transponders des Hundes sowie die zuständige Behörde zum Abruf bereitgestellt werden. Im Trefferfall kann dann Kontakt mit dieser Behörde aufgenommen und die weiteren erforderlichen Daten können bilateral ausgetauscht werden. Der Begründung des Verordnungsentwurfs war zu entnehmen, dass der Hauptgrund für die zuverlässige Ermittlung des Halters aus ordnungsrechtlicher Sicht darin liege, diesen im Einzelfall zur Verantwortung zu ziehen. Eine Notwendigkeit für eine sofortige Ermittlung des Halters ist aus der Begründung aber nicht ersichtlich. Sofern es zu Beißattacken kommen sollte, werden ohnehin zunächst von der Polizei Sofortmaßnahmen gegen den Hund ergriffen, sodass eine sofortige Ermittlung des Halters aus Gründen der Gefahrenabwehr nicht erforderlich ist. Der vorgelegte Verordnungsentwurf stellte keine, wie in der Begründung erwähnt, datensparsame Regelung dar. Erst mit der Streichung der Halterdaten aus dem zentralen Register, wie dies z. B. in Nordrhein-Westfalen praktiziert wird, könnte der Grundsatz der Datensparsamkeit Beachtung finden.

Darüber hinaus wäre eine zentrale Registrierung sämtlicher Hundehalterdaten, unabhängig davon, ob deren Hunde als gefährlich einzustufen sind, als nicht mehr angemessen anzusehen. Dies ergibt sich aus der mit der zentralen Registrierung in § 3 des Entwurfs sowie der in § 4 des Entwurfs vorgesehenen Abrufmöglichkeit durch eine Vielzahl von Behörden und der damit verbundenen erhöhten Missbrauchsgefahr für diese Daten, der auf der anderen Seite keine zwingende Notwendigkeit für die zentrale Zur-Verfügung-Stellung gegenübersteht.

Der TLfD teilte dem TIM mit, dass er das Risiko der Verfassungswidrigkeit der geplanten Regelung zur Einführung eines zentralen Hundehalterregisters für nicht unerheblich hält und daher empfiehlt, darauf im Verordnungswege zu verzichten. Ggf. sollte eine gesetzliche Grundlage für ein reines Hunderegister (ohne Halterdaten) im Thüringer Gesetz zum Schutz der Bevölkerung vor Tiergefahren angestrebt werden. Vom TIM werden diese Bedenken aufgenommen.

6 Personaldaten

6.1 Beschäftigtendatenschutz immer noch nicht geregelt

Im 8. Tätigkeitsbericht (6.1) hatte der TLfD über die Forderung nach Schaffung von klaren Regelungen zum Umgang mit personenbezogenen Daten, die bei der Begründung, Durchführung, Beendigung und Abwicklung von Arbeitsverhältnissen erhoben und gespeichert werden, berichtet. Diesem Anliegen kam der Landesgesetzgeber mit einer Neuregelung in § 33 ThürDSG nach. Die Bundesregierung hat am 25. August 2010 den Entwurf eines Beschäftigtendatenschutzgesetzes beschlossen und in die parlamentarische Beratung eingebracht (BT-Drs. 17/4230). Nachdem der Bundesrat am 5. November 2010 hierzu Stellung genommen hatte, wurde der Gesetzentwurf am 25. Februar 2011 im Bundestag in erster Lesung beraten und an den federführenden Innenausschuss sowie die mit beratenden Ausschüsse überwiesen. Am 23. Mai 2011 fand im Innenausschuss des Deutschen Bundestages eine Sachverständigenanhörung statt. Ob der Regierungsentwurf im weiteren Gesetzgebungsverfahren nachgebessert wird, ist derzeit nicht abzusehen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (Anlage 13) anlässlich ihrer 81. Konferenz am 16./17. März 2011 an den Gesetzgeber appelliert, notwendige Anforderungen zum Beschäftigtendatenschutz sicherzustellen. So sind restriktive normenklare Regelungen zu Eignungstests und medizinischen Untersuchungen, zu Screening-Verfahren, zur betrieblichen Videoüberwachung sowie zur Erhebung und Nutzung von Beschäftigtendaten zur Aufdeckung von Pflichtverletzungen erforderlich. Auch ist eine Datenerhebung zum Zwecke der Verhaltens- und Leistungskontrolle nur insoweit als zulässig anzusehen, soweit sie nicht zu einem unzumutbaren Überwachungsdruck führt. Eine verdeckte Überwachung sollte nur dann durchgeführt werden dürfen, wenn dokumentierte Tatsachen für Straftaten und Pflichtverletzungen vorliegen. Auch sind Stellenbewerber so früh wie möglich über die Datenerhebung aus allgemein zugänglichen Quellen, wie dem Internet, zu unterrichten. Des Weiteren wurde darauf hingewiesen, dass die Wahrnehmung des „Petitionsrechts“ nicht beschränkt werden darf. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemäßigelt zu werden. Schließlich wurde Rege-

lungsbedarf für wichtige Bereiche des Beschäftigtendatenschutzes wie der Personalaktenführung, einschließlich der automatisierten Verfahren, der „gemischten“ dienstlichen und privaten Nutzung von Telekommunikationsdiensten, dem Whistleblowing, der Videoüberwachung im öffentlich zugänglichen Bereich, bei der auch Beschäftigtendaten anfallen, einem Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung und dem Konzerndatenschutz einschließlich des internationalen Datenverkehrs geltend gemacht.

Angesichts der bekannt gewordenen Datenskandale kommt es darauf an, dass das erklärte Ziel des Gesetzgebers, die Arbeitnehmer vor einer unrechtmäßigen Erhebung und Verwendung ihrer Daten zu schützen, durch baldige Verabschiedung eines umfassenden, sachgerechten und normenklaren Beschäftigtendatenschutzgesetzes verwirklicht wird.

6.2 Umgang mit amtsärztlichen Gutachten

Der Umgang mit amtsärztlichen Gutachten führt immer wieder zu Fragen an den TLfD. So bat z. B. ein Landratsamt um Prüfung datenschutzrechtlicher Aspekte im Zusammenhang mit einer gerichtlichen Auseinandersetzung um die Versetzung eines Beamten in den Ruhestand wegen Dienstunfähigkeit. Der Betroffene hatte den ursprünglich zuständigen Amtsarzt und die behandelnden Ärzte gegenüber dem Amtsarzt nicht von ihrer Schweigepflicht gemäß § 203 StGB entbunden. In Folge dessen konnten die Diagnosen zu früheren Behandlungen nicht in das aktuelle amtsärztliche Gutachten einbezogen werden. Nach Auffassung des Gerichtes reichten die Aussagen des vorliegenden amtsärztlichen Gutachtens nicht dazu aus, um eine Versetzung in den Ruhestand zu rechtfertigen. Seitens des TLfD wurde in diesem Zusammenhang auf Folgendes hingewiesen:

Der Umfang der Offenbarungsbefugnis des Arztes gegenüber der anfordernden Behörde richtet sich nach § 47 Abs. 1 ThürBG, wonach die tragende Gründe und Feststellungen enthaltenden Gutachten nur soweit mitgeteilt werden dürfen, wie deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für ihre zu treffende Entscheidung erforderlich ist. Dies bedeutet jedoch nicht, dass ein Amtsarzt nicht zur Dokumentation der tragenden medizinischen Untersuchungsbefunde verpflichtet ist. Diese

Dokumentation ist beim Arzt selbst zu führen und unterliegt der Schweigepflicht. Die anfordernde Behörde kann keine eigene medizinische Beurteilung zur Dienstfähigkeit eines Beamten vornehmen, sodass eine detaillierte Begründung des Gutachtenergebnisses unter Benennung von Diagnosen und Vorerkrankungen nicht erforderlich ist. Vielmehr muss sich der begutachtende Arzt auf die Beantwortung von konkreten Fragen der Behörde beschränken. Welche Anforderungen die Behörden des Landes bei Gutachtaufträgen an die Amtsärzte zu beachten haben, ist aus den „Empfehlungen für das Verfahren bei längerfristigen Erkrankungen, Wiedereingliederung und Frühpensionierung“ zu entnehmen, die in einer ressortübergreifenden Arbeitsgruppe erarbeitet und vom TIM an die Behörden zur Kenntnis gegeben worden ist.

In einem weiteren Fall sah sich der TLfD veranlasst, gemäß § 37 ThürDSG aufgrund einer Beschwerde eines Kommunalbeamten wegen des Umgangs mit einem amtsärztlichen Gutachten und einer Aufstellung seiner Krankheitsstage, Einblick in die Personalakte des Betroffenen beim Kommunalen Versorgungsverband Thüringen zu nehmen. Bewertungsmaßstab dieser datenschutzrechtlichen Kontrolle war der Grundsatz, dass nur solche Unterlagen und Daten in die Personalakte aufgenommen werden dürfen, die im unmittelbaren Zusammenhang mit dem Dienstverhältnis stehen, § 50 Beamtenstatusgesetz und § 89 ThürBG. Die Personalaktenführung in öffentlichen Stellen des Landes richtete sich, da § 33 ThürDSG noch nicht in Kraft war, auch für den Angestelltenbereich mangels konkreter bereichsspezifischer Regelungen nach den dienstrechtlichen Vorschriften für Beamte. So sind die Unterlagen der Personalakte zu amtsärztlichen Gutachten auf die zulässigen Feststellungen „dienstfähig“, „dienstunfähig“ oder „eingeschränkt dienstfähig“ zu beschränken. Nur im letzteren Fall sind Ergänzungen zu weiterem Handlungsbedarf der Dienststelle notwendig. Nicht zulässig sind insbesondere die Mitteilung von Diagnosen und Angaben zu sonstigen behandelnden Ärzten. Amtsärztliche Gutachten, die Angaben enthalten, die gemäß §§ 47 ff. ThürBG nicht vorgesehen sind, sind an den Amtsarzt zurückzugeben und es sind im Umfang beschränkte Feststellungen anzufordern. Diese Unterlagen sind in Umschlägen, die entsprechend 3.2, 4. Absatz der Personalaktenführungsrichtlinie (ThürStAnz 1998, 1812 ff.) gekennzeichnet sind, aufzubewahren. Unterlagen, die die Häufigkeit und die Art der

Arztbesuche über einen gewissen Zeitraum dokumentieren, wie Kopien von Arztterminzetteln, sind nicht für die Personalakte geeignet und daher zu entfernen. Die kontrollierte Personalakte wurde entsprechend der Forderungen des TLfD überarbeitet und es wurde angekündigt, dass sämtliche beim Kommunalen Versorgungsverband Thüringen geführten Personalakten bis Ende 2011 entsprechend überarbeitet werden.

Der Arzt darf der anfordernden Behörde die tragende Gründe und Feststellungen enthaltenden Gutachten nur soweit mitteilen, wie deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für ihre zu treffende Entscheidung erforderlich ist.

Es sind nur solche Unterlagen in die Personalakte aufzunehmen, die im unmittelbaren Zusammenhang mit dem Dienstverhältnis stehen. So sind die Unterlagen der Personalakte zu amtsärztlichen Gutachten auf die zulässigen Feststellungen „dienstfähig“, „dienstunfähig“ oder „eingeschränkt dienstfähig“ zu beschränken.

6.3 Umgang mit Personalunterlagen zur Stasiüberprüfung in der Thüringer Polizei

In den Medien wurde berichtet, dass Personalunterlagen zu Stasi-Überprüfungen der Polizei über mehrere Jahre illegal gelagert worden seien. Um diesen Vorwurf aus datenschutzrechtlicher Sicht zu überprüfen, erfolgten Vorortbesuche bei der Bereitschaftspolizei Thüringen an verschiedenen Standorten. Da der fragliche Aktenbestand zunächst auf Anordnung der Staatsanwaltschaft Erfurt im Rahmen eines strafrechtlichen Ermittlungsverfahrens sichergestellt und ausgewertet wurde, ist erst nach Beendigung dieser Maßnahmen eine Einsichtnahme in den Aktenbestand erfolgt. Die stichprobenhafte Einsichtnahme in den Aktenbestand hat ergeben, dass es sich bei den Unterlagen um Stasi-Überprüfungsakten von ehemaligen Angehörigen der Deutschen Volkspolizei handelt, die zunächst in den Dienst der Landespolizei Thüringen übernommen worden und nach einer positiven (belastenden) Gauck-Auskunft sowie einer anschließenden Einzelfallüberprüfung ausgeschieden sind. Ein kleinerer Teil der Akten enthielt Unterlagen des TIM, die zur Prozessführung bei Klagen der Betroffenen gegen ihre Entlassung separat angelegt wurden. Diese Akten wurden im TIM angelegt und bis zum

Jahr 2005 auch dort gelagert. Die Stasi-Überprüfungsakten von weiterbeschäftigten Polizeibeamten werden nach wie vor im TIM aufbewahrt. 1997 wurde mit Auflösung des Polizeipräsidiums die Zuständigkeit für die Personalakten ausgeschiedener Polizeibeamter auf die Rentenstelle beim Thüringer Polizeiverwaltungsamt verlagert. Zunächst wurden die Überprüfungsakten vom TIM als Sachakten angesehen und weiterhin im TIM gelagert. Im Jahr 2005 kam das TIM zu der Überzeugung, dass die Stasi-Überprüfungsakten als Teil der Personalakte anzusehen sind. Im gleichen Jahr wurden die Akten der wegen Stasi-Belastung gekündigten Bediensteten in 78 Ordnern gegen Übergabebescheinigung der Rentenstelle beim Polizeiverwaltungsamt übergeben und in einem ständig bewachten Gebäude untergebracht. Nach Auflösung des Polizeiverwaltungsamts ging die Rentenstelle zum 1. Mai 2008 an die Bereitschaftspolizei über, wobei die Überprüfungsakten zunächst am bisherigen Standort verblieben. Aufgrund des Wegfalls der ständigen Bewachung des Gebäudes wegen des Auszugs der dortigen Polizeiinspektion wurde der Aktenbestand am 23. Mai 2008 in einen fensterlosen Raum der Bereitschaftspolizei gebracht. Dieser Raum, über dessen Schlüssel nur der Leiter der Bereitschaftspolizei und dessen Stellvertreter verfügte, wurde verschlossen und versiegelt. Nach einer erneuten Überprüfung innerhalb der Bereitschaftspolizei wurde der Aktenbestand am 1. April 2011 in das Aktenlager der Rentenstelle in Kellerräume der Polizeiinspektion Erfurt-Nord verbracht. In einem gesondert abschließbaren Raum waren dort bereits die Personalakten der ausgeschiedenen Bediensteten der Thüringer Polizei gelagert. Zutrittsberechtigt waren nur der Leiter und zwei Mitarbeiter der Rentenstelle.

Es konnten keine schwerwiegenden Verletzungen datenschutzrechtlicher Vorschriften im Umgang mit den Stasi-Überprüfungsakten festgestellt werden. Insbesondere sind die Umstände der Lagerung und die Zugriffsrechte als dem Schutzbedürfnis dieser Unterlagen angemessen anzusehen. Generell sind solche Akten auch Bestandteil von Personalakten, die so lange wie die Personalakte selbst aufzubewahren sind. Mängel haben sich insoweit gezeigt, als der Aktenbestand bislang nicht dahingehend überprüft wurde, ob die Aufbewahrungsfristen im Einzelfall abgelaufen und die Akten den zuständigen Staatsarchiven angeboten werden müssen. Außerdem waren in den Personalgrundakten keine ausreichend konkreten Verweise auf

die an einem anderen Ort besonders gesicherten Stasi-Überprüfungsakten enthalten.

Stasi-Überprüfungsakten sind Teil der Personalakte. Wegen ihres sensiblen Inhalts sind sie in einer gegen unbefugten Zugriff besonders gesicherten Teilakte zu führen. Um diese Sicherheit zu gewährleisten, kann die Teilakte auch an einen besonders geschützten Ort verbracht werden. Hierauf muss allerdings aus Gründen der Transparenz in der Personalakte hingewiesen werden. Selbst wenn der Umgang mit Unterlagen zur Stasi-Überprüfung von den zuständigen Stellen als sehr sensibel angesehen wird, dürfen diese Unterlagen nicht ungeprüft weggeschlossen werden. Unter Beachtung der notwendigen Maßnahmen gegen unbefugten Zugriff müssen diese Unterlagen entsprechend den Vorschriften der Personalaktenführungsrichtlinie behandelt werden.

6.4 Videoüberwachung in den Pausenräumen der Uniklinik Jena

Ein Mitarbeiter der Uniklinik Jena beschwerte sich über eine verdeckte bzw. heimliche Videoüberwachung von Pausenräumen des dortigen Operationsbereichs. Es wurde festgestellt, dass im September 2009 in der Klinik Videokameras installiert wurden, deren Verkleidung die Aufschrift „Alarmanlage“ trug. Ein Hinweisschild auf die Videoüberwachung war nicht vorhanden. Dem Betroffenen war von einem leitenden Klinikmitarbeiter zunächst gesagt worden, dass es sich dabei lediglich um Klimatechnik handele. Wie die Uniklinik auf Anfrage des TLfD mitteilte, sei die Videoüberwachung zur Aufklärung einer großen Zahl von Diebstählen im Umfeld der Operationssäle veranlasst worden. Nach den von der Rechtsprechung entwickelten Maßstäben ist eine heimliche Videoüberwachung nur dann als zulässige arbeitsrechtliche Maßnahme anzusehen, wenn ein Verdacht auf eine oder wenige Personen begrenzt werden kann. Da der Diebstahlsverdacht jedoch im Ergebnis der Ermittlungen nicht auf bestimmte Personen begrenzt werden konnte, war die durchgeführte heimlich Videoüberwachung als datenschutzrechtlicher Verstoß anzusehen.

Der TLfD forderte, die Dienstvereinbarung zum Einsatz von Videotechnik zwischen der Leitung der Uniklinik und dem Personalrat so

zu überarbeiten, dass eindeutig erkennbar ist, welche konkreten Video- und Audioüberwachungssysteme für welche Zwecke eingesetzt werden können, ob und für welche Zwecke Videoaufzeichnungen genutzt werden dürfen und welche konkreten technischen und organisatorischen Maßnahmen zum Ausschluss einer Verhaltens- und Leistungskontrolle von Beschäftigten sowie zur Sicherstellung der datenschutzrechtlichen Vorschriften, insbesondere um unbefugten Zugriff auszuschließen, getroffen wurden. Bislang steht der Abschluss einer überarbeiteten Dienstanweisung noch aus, da Einzelheiten noch mit dem Personalrat ausgehandelt werden. Die Leitung der Uniklinik versicherte dem TLfD allerdings, dass keine heimliche Videoüberwachung am Universitätsklinikum durchgeführt wird.

Nach den von der Rechtsprechung entwickelten Maßstäben ist eine heimliche Videoüberwachung nur dann als zulässige arbeitsrechtliche Maßnahme anzusehen, wenn ein Verdacht auf eine oder wenige Personen begrenzt werden kann.

7 Polizei

7.1 Körperscanner nur mit Datenschutz

Die Sicherheit im Flugverkehr wurde in den vergangenen Jahren immer wieder auf den Prüfstand gestellt, sei es durch das Verbot von Flüssigkeiten im Handgepäck oder die vorherige Durchsuchung der Reisenden. So hat nach einem Anschlagversuch in Detroit Ende 2009 eine öffentliche Diskussion um den Einsatz von sogenannten Nacktscannern viele Fragen zum Schutz der Persönlichkeitsrechte der Passagiere aufgeworfen. Dabei ging es vor allem darum, dass durch den Einsatz von Detektionsgeräten ein realistisches Abbild der Körperkonturen angezeigt werden kann, das die Betroffenen in ihrem Schamgefühl und damit in ihrer Menschenwürde verletzen könnte. Zudem können mit derartigen Scannern grundsätzlich auch körperliche Anomalien wie z. B. künstliche Körperteile oder medizinische Hilfsmittel (wie Prothesen oder künstliche Darmausgänge) angezeigt werden, die normalerweise unter der Kleidung nicht sichtbar sind. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (Anlage 4) gefordert, dass der Gesetzgeber vor dem Einsatz solcher Geräte datenschutzrechtliche Bedingungen formulieren muss, um Beeinträchtigungen der Persönlichkeitsrechte weitgehend auszuschließen. Dazu gehört zunächst die Prüfung, ob mit den Geräten tatsächlich ein nennenswerter Sicherheitsgewinn erzielbar ist. Ist dies der Fall, so muss sichergestellt werden, dass eine Anzeige der Körperkonturen (kein Nacktscanner) unterbleibt und eine Speicherung der Daten über den Kontrollvorgang ausgeschlossen wird. Schließlich muss auch sichergestellt werden, dass die Menschenwürde gewahrt bleibt und künstliche Körperteile oder medizinische Hilfsmittel nicht angezeigt werden.

Körperscanner werden von der Thüringer Polizei nicht genutzt; vor ihrem Einsatz müssen die rechtlichen Rahmenbedingungen unter Beachtung der Persönlichkeitsrechte der Betroffenen durch den Gesetzgeber festgelegt werden.

7.2 Datenverarbeitungen beim Papstbesuch

Die umfangreichen Sicherheitsmaßnahmen beim Besuch des Papstes in Thüringen im September 2011 führten auch zur Verarbeitung personenbezogener Daten im Vorfeld der Visite. So wurde der TLfD auf das Besucheranmeldeverfahren aufmerksam. Dabei erfolgte für die Teilnahme an den Gottesdiensten eine Anmeldung über das Internet, bei der neben dem Namen auch eine Angabe zu Geburtsdatum, Geburtsort, Anschrift und E-Mail-Adresse verlangt wurde. Da diese Datenerhebung durch die katholische Kirche erfolgte, lag dies nicht im Zuständigkeitsbereich des TLfD. Allerdings wurde die Erhebung dieser Daten auf der Internetseite zum Papstbesuch (www.papst-in-deutschland.de) zunächst auch mit den Sicherheitsanforderungen der Polizei begründet. Daher fragte der TLfD beim TIM nach, ob und zu welchem Zweck die Thüringer Sicherheitsbehörden personenbezogene Daten aus den Anmeldungen der Gottesdienstbesucher erhalten sollen. In einem daraufhin geführten Gespräch mit dem Vorbereitungsstab der Polizei wurde klargestellt, dass die von der katholischen Kirche zur Kartenvergabe erhobenen Daten nicht an die Polizei übermittelt werden. Kurz darauf hat die katholische Kirche auf die Erhebung dieser Daten verzichtet und bereits erhobene Daten gelöscht. Gleichwohl wurden vor dem Papstbesuch durch die Polizei persönliche Daten zur Gefahrenvorsorge erhoben und verarbeitet. Dabei kam zum wiederholten Mal ein Akkreditierungsverfahren zur Anwendung, das bereits bei der Fußball WM 2006 eingesetzt wurde und damals als nur einmalige Aktion bezeichnet worden war (vgl. 7. TB, 7.3 sowie 8. TB, 7.4). Tatsächlich scheint sich diese Verfahrensweise jedoch allmählich zu einer polizeilichen Standardmaßnahme herauszubilden. Danach mussten sich alle Personen, die sich dem Papst auf mehr als 30 Meter nähern können, einer Zuverlässigkeitsüberprüfung unterziehen. Im Nahbereich bis etwa 5 Meter um den Papst erfolgte die Prüfung durch das Bundeskriminalamt. Die betreffenden Personen erhielten dazu eine datenschutzrechtliche Erklärung, die über das vorgesehene Verfahren informiert, und sollten dann ihre schriftliche Einwilligungserklärung erteilen, dass die Sicherheitsbehörden ihre Zuverlässigkeit (insbesondere durch Abgleich mit den hierzu bestehenden Datenbanken) überprüfen dürfen. Die Polizei teilte dann der katholischen Kirche lediglich das Ergebnis der Prüfung in Form einer Empfehlung (Akkreditierung ja oder nein) mit. Dem TIM wurde mitgeteilt, dass

es der TLfD nach wie vor kritisch sehe, wenn derartige Zuverlässigkeitsüberprüfungen ohne eine dem Verhältnismäßigkeitsgrundsatz entsprechend gesetzliche Grundlage allein auf Grundlage der Einwilligungen der Betroffenen durchgeführt werden.

Wie bereits mehrfach angemahnt, dürfen derartige Zuverlässigkeitsprüfungen nicht regelmäßig auf Einwilligungserklärungen der Betroffenen gestützt werden. Bei einem künftigen Bedarf ist daher eine Rechtsgrundlage zu schaffen.

7.3 Unzulässige Zuverlässigkeitsprüfung auch noch mit veralteten Daten

Welche Folgen ein nicht sorgfältiger Umgang mit Daten aus polizeilichen Datenbanken haben kann, wurde an der Beschwerde einer Frau deutlich, der auf Vermittlung der ARGE eine Arbeitsgelegenheit bei einem Verein angeboten wurde. Ihre Aufgabe sollte es sein, Kinder zur Erhöhung der Schulwegsicherheit in den Schulbussen zu begleiten. Nach nur kurzer Tätigkeit wurde vom Verein die Vereinbarung mit der Begründung gekündigt, dass von polizeilicher Seite die Ungeeignetheit für die Aufgaben zum Einsatz als Schulbusbegleiter mitgeteilt worden sei. Als sie bei dem Verein nachfragte, wie die Polizei überhaupt zu einer solchen Einschätzung käme, wurde ihr Erstaunliches mitgeteilt. Danach sei es eine gängige Praxis, dass sämtliche Verkehrshelfer zu Beginn des Einsatzes vom Verein an die Polizei gemeldet werden. Diese überprüfe dann, ob bei den Betroffenen eventuelle Vorstrafen vorliegen und äußere dann nach Prüfung eventuelle Bedenken gegen die beabsichtigte Tätigkeit. Eine darauf bei der Polizeiinspektion Kyffhäuser erfolgte Nachfrage der Betroffenen nach den Gründen für die Eignungsbedenken wurde mitgeteilt, es habe drei Einträge im Datenbestand von INPOL (Informationssystem der Polizei) zu Ermittlungsverfahren wegen Verletzung der Fürsorge- und Erziehungspflichten, Misshandlung von Schutzbefohlenen sowie Beleidigung und Verleumdung gegeben. Wegen des beabsichtigten Umgangs mit Kindern als Schulbusbegleiter bestünden bei diesen Tatvorwürfen aus den vorangegangenen Ermittlungsverfahren Bedenken gegen die Ausübung der Tätigkeit. Da alle Ermittlungsverfahren gegen die Frau nach § 170 Abs. 2 StPO eingestellt worden sind, wandte sie sich an den TLfD mit der Bitte um Prüfung, ob diese Verfahrensweise als rechtmäßig anzusehen ist.

Wie sich nach einer Prüfung ergab, war sie es aus drei Gründen nicht. Bereits fraglich ist, ob die Übermittlung der Daten der Frau ohne ihre Einwilligung von dem Verein an die Polizei zulässig ist. Dies war jedoch im Jahr 2010 vom TLfD noch nicht zu prüfen, da hierfür das Landesverwaltungsamt zuständige Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich war. Der erste Verstoß gegen datenschutzrechtliche Vorschriften war in einem unzulässigen Abgleich der Daten der Betroffenen mit den polizeilichen Dateien zu sehen. Entgegen der Auffassung der Polizei lagen hier nicht die Voraussetzungen von § 43 Abs. 1 Satz 2 PAG vor. Danach ist ein Datenabgleich von Nichtstörern nur dann zulässig, wenn dies aufgrund tatsächlicher Anhaltspunkte zur Erfüllung polizeilicher Aufgaben geboten erscheint. Der beabsichtigte Einsatz von Verkehrshelfern in Schulbussen stellt für sich keine abstrakte oder konkrete Gefahr für polizeiliche Schutzgüter dar, solange keine allgemeinen oder konkreten tatsächlichen Anhaltspunkte für eine solche Gefahr vorliegen. Hier sollte der Abgleich gerade erst dazu dienen, Anhaltspunkte für eine mögliche Gefährdung der Kinder durch den Einsatz der vorgesehenen Verkehrshelfer zu gewinnen. Eine weitere Verletzung datenschutzrechtlicher Vorschriften lag darin, dass die beim Datenabgleich ermittelten INPOL-Eintragungen nicht bereits nach Mitteilung der Verfahrenseinstellung gemäß § 40 Abs. 2 Satz 5 PAG gelöscht worden sind. Die Überprüfung durch die PD Nordhausen hatte ergeben, dass es versäumt wurde, beim Eingang der Verfahrenseinstellung im Jahr 2008 die schriftliche Einstellungsverfügung daraufhin zu prüfen, ob eine weitere Speicherung der Erkenntnisse erfolgen darf. Wäre diese Prüfung erfolgt, so hätte es überhaupt keinen Treffer gegeben. Schließlich lag ein dritter Verstoß gegen datenschutzrechtliche Vorschriften in der Übermittlung des Ergebnisses der „Zuverlässigkeitsprüfung“ an den Verein, ohne dass hierfür die Voraussetzungen des § 41 Abs. 3 Satz 2 PAG vorlagen. Eine solche Übermittlung wäre nur zulässig, wenn dies zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder für die schutzwürdigen Belange Einzelner erforderlich ist. Es war hier nicht im Ansatz erkennbar, welche erheblichen Nachteile den Kindern durch die Tätigkeit der Frau als Verkehrshelferin z. B. durch Schulbusbegleitung, Sicherung an Überwegen und an Bushaltestellen oder Begleitung bei Verkehrsschulungen etc. entstehen sollten. Außer den unrichtigen INPOL-

Einträgen gab es für die Polizei keine weiteren Anhaltspunkte, dass durch die Tätigkeit der Frau eine Gefahr für die betreuten Kinder ausgeht. Der TLfD hat diese Verletzungen von datenschutzrechtlichen Vorschriften formell nach § 39 Abs. 1 ThürDSG beanstandet und von der Polizei gefordert, darauf hinzuwirken, dass bereits keine solchen Listen mehr von Vereinen an die Polizei übersandt werden. Außerdem wurde die Polizei aufgefordert, mit Einverständnis der Frau dem Verein mitzuteilen, dass die geäußerten Bedenken gegen eine Tätigkeit der Frau von Anfang an unbegründet waren. Dem ist die Polizeiinspektion Kyffhäuser nachgekommen. Daneben hat das TIM die ungeprüfte Abfrage und Weitergabe von eigentlich zu löschenden Eintragungen im INPOL zum Anlass dafür genommen, in einem Erlass an alle Polizeidienststellen darauf hinzuweisen, dass vor einer Übermittlung von Erkenntnissen die Aktualität und Vollständigkeit der Daten zu überprüfen ist. Außerdem wurde darauf hingewiesen, dass eine Übermittlung an nicht-öffentliche Stellen nach § 41 PAG nur in absoluten Ausnahmefällen zulässig sein kann.

Der Fall zeigt, dass die Folgen einer unzulässigen Datenübermittlung umso gravierender sein können, wenn die Aktualität der automatisiert gespeicherten Daten nicht sorgfältig geprüft wird. Das Anliegen, den Schutz von Kindern in Ihrem Umfeld zu gewährleisten, sollte nicht durch wahlloses Recherchieren in polizeilichen Datenbanken erfolgen. Vielmehr sollte vom Instrument eines erweiterten Führungszeugnisses nach § 30 a Bundeszentralregistergesetz (BZRG) Gebrauch gemacht werden, das auch Vereine von Bewerbern verlangen können, wenn diese bei ihrer Tätigkeit mit Minderjährigen in Kontakt kommen.

7.4 Kein Datenabgleich zur Verdachtsgewinnung

Durch eine Beschwerde wurde der TLfD auf eine Verfahrensweise der Thüringer Polizei bei der Abfrage von Daten aus polizeilichen Dateien aufmerksam, die nach Auffassung des TLfD nicht mit den gesetzlichen Vorgaben des PAG in Einklang zu bringen ist. Im konkreten Fall hatte die Polizeidirektion Erfurt an einem sogenannten gefährlichen Ort nach § 14 Abs. 1 Satz 2 PAG eine Identitätskontrolle von Radfahrern vorgenommen. Der Betroffene wurde dort angehalten und nach Feststellung seiner Identität wurden ohne weitere Prüfung seine personenbezogenen Daten nicht nur mit dem

Fahndungsbestand sondern mit sämtlichen polizeilichen Dateien abgeglichen. Erst durch eine dann erfolgte Treffermeldung in der polizeilichen Verbunddatei „Kriminalaktennachweis“ zu einem früheren Vergehen nach dem Betäubungsmittelgesetz ergaben sich weitere Anhaltspunkte für eine Überprüfung des Betroffenen. § 43 Abs. 1 Satz 1 PAG erlaubt einen Abgleich mit dem Inhalt sämtlicher polizeilicher Dateien nur bei Verhaltens- und Zustandsstörern (§§ 7 und 8 PAG). Nach § 43 Abs. 1 Satz 3 PAG ist im Rahmen der Aufgabenerfüllung ein Datenabgleich ohne Einschränkung auf eine besondere Qualität von Störern jedoch nur hinsichtlich des Fahndungsbestandes, d. h. derjenigen Personen, die zur Fahndung ausgeschrieben sind, möglich. Das bedeutet, dass ein Abgleich mit allen polizeilichen Dateien bei Personen, die nicht auffällig geworden sind oder die Verantwortung für eine Gefahrensituation tragen, allein zur Verdachtsschöpfung nicht zulässig ist. Daher setzt § 43 Abs. 1 Satz 2 PAG für einen Abgleich mit sämtlichen polizeilichen Datenbanken von Nichtstörern voraus, dass tatsächliche Anhaltspunkte vorliegen, die einen solchen Abgleich zur Erfüllung polizeilicher Aufgaben als geboten erscheinen lassen. Obwohl dies keine besonders hohen Hürden sind, bedarf es nach Auffassung des TLfD zumindest der Prüfung, ob es im konkreten Einzelfall solche tatsächlichen Anhaltspunkte gibt. Die Polizeidirektion Erfurt und das daraufhin vom TLfD zur Stellungnahme aufgeforderte TIM waren dagegen der Auffassung, dass hierfür bereits die Anwesenheit an einem gefährlichen Ort im Sinne des § 14 Abs. 1 Nr. 2 PAG ausreiche, ohne dass es weiterer tatsächlicher Anhaltspunkte bedarf. Das TIM sieht als tatsächliche Anhaltspunkte zur Erfüllung polizeilicher Aufgaben die Anwesenheit der Personen an einem gefährlichen Ort oder in der Nähe eines gefährdeten Objekts als ausreichend an. Der Wortlaut des § 43 Abs. 1 Satz 2 PAG enthält jedoch keinen Hinweis darauf, dass es für einen Datenabgleich genügt, dass eine Person an einem gefährlichen Ort angetroffen wird. Diese sogenannte „Ortschaftung“ begründet nach § 14 Abs. 1 Nr. 2 PAG nur die Befugnis der Polizei zur Feststellung der Identität einer Person. Will die Polizei während oder nach der Identitätsfeststellung sämtliche polizeiliche Dateien mit dem Namen der angetroffenen Person abgleichen, genügt nicht allein das Antreffen der Person an einem gefährlichen Ort. Vielmehr müssen auf die konkrete Person bezogen tatsächliche Anhaltspunkte vorliegen, die einen Datenabgleich zur Erfüllung polizeilicher Aufgaben geboten erscheinen lassen. Wie aus

der Antwort der Landesregierung auf die Kleine Anfrage 1780 (LT-Drs. 5/3433) zu Frage 2 hervorgeht, hat es mit Vertretern des TIM ein Gespräch zum weiteren Vorgehen gegeben. Dabei konnten die unterschiedlichen Standpunkte nicht ausgeräumt werden. Das TIM wurde aufgefordert, die rechtswidrige Datenabgleichspraxis bei der Thüringer Polizei einzustellen.

Das TIM muss bei der Thüringer Polizei dafür sorgen, dass die aus Sicht des TLfD rechtswidrige Praxis des Abgleichs der Daten von Nichtstörern mit allen polizeilichen Datenbanken ohne konkrete tatsächliche Anhaltspunkte in der Person des Betroffenen eingestellt wird.

7.5 Neugier von Kollegen

Ein gewisser Wissensdurst ist für jeden Polizisten Grundvoraussetzung zur Erledigung seiner täglichen Aufgaben. Manchmal richtet sich dieser aber auch auf Gegenstände, die nur am Rande etwas mit den polizeilichen Aufgaben zu tun haben. So war es in einem Fall, bei dem ein Polizeibeamter selbst mit dem Gesetz in Konflikt geraten war und sein abgeurteiltes Vergehen im INPOL gespeichert wurde. Da er vermutete, dass sich seine Kollegen unbefugt Kenntnis über seinen Eintrag verschafft haben könnten, wandte er sich an den TLfD mit der Bitte um Überprüfung. Eine Auswertung der Protokolldaten der letzten 12 Monate durch das TLKA für den TLfD hat ergeben, dass von über 30 Personen auf den Datensatz des Polizeibeamten in INPOL zugegriffen worden war. Ein daraufhin durchgeführter Kontrollbesuch in der Polizeidirektion Gotha hat dieses Ergebnis bestätigt. Die für den Polizeibeamten zuständige Dienststelle hatte parallel zum TLfD ebenfalls eine Protokolldatenrecherche beim TLKA durchgeführt und diese zusätzlich auf Zugriffe auf das Integrationsverfahren der Polizei (IGVP), erstreckt, in dem u. a. die Vorgangsverwaltung enthalten ist. Die Zahl derjenigen, die auf Datensätze des betreffenden Polizeibeamten in beiden Verfahren zugegriffen hatten, lag noch um einiges höher als die vom TLfD festgestellten Zugriffe. Dabei wurde auch festgestellt, dass der betreffende Beamte selbst mehrfach auf die über ihn in den polizeilichen Datenbanken gespeicherten Daten zugegriffen hat.

In einem nächsten Schritt war nun zu prüfen, in welchen Fällen die nachgewiesenen Zugriffe zur Erfüllung der Aufgaben des jeweiligen Beamten erforderlich waren, denn nur dann handelt es sich um eine rechtlich zulässige Nutzung personenbezogener Daten. Allein die Anzahl der Zugriffe ließ es als sehr unwahrscheinlich erscheinen, dass alle diese Zugriffe zur Aufgabenerfüllung erforderlich waren. Eine Befragung der Betroffenen durch deren Vorgesetzte hat dann ergeben, dass ein Teil der Beamten eine dienstliche Erforderlichkeit darlegen konnte. Ein anderer Teil hat eingeräumt, die Daten aus reiner Neugier abgerufen zu haben. Schließlich blieb auch hier ein Teil der Beamten übrig, die sich nicht mehr an den Abruf erinnern konnten. Hier zeigten sich erneut die Schwächen der unzureichenden Protokollierung, die nicht zwingend vorsieht, dass bei der Abfrage der Grund der Abfrage angegeben werden muss (vgl. 8. TB, 7.6). Allerdings lag hier der Rechtfertigungsdruck höher, da es sich um Daten eines Kollegen handelt, bei deren Abfrage die Erinnerung evtl. nicht so schnell verblassen dürfte.

Sofern kein dienstlicher Anlass zur Abfrage der Daten vorlag und diese aus reiner Neugier erfolgte, ist eine solche Abfrage als unbefugte Nutzung unter Verletzung von § 40 Abs. 1 PAG anzusehen. Nicht nur der Zugriff durch die Kollegen ist als Verletzung datenschutzrechtlicher Vorschriften einzuordnen, dies gilt auch für die Zugriffe des betroffenen Beamten auf die zu seiner Person gespeicherten Daten, sozusagen als „Selbstauskunft“. Wenn also die Datenabfragen ausschließlich dazu gedient haben, dass er erfährt, ob seine Vergehen in den polizeilichen Datensammlungen erfasst sind oder nicht, dann stellt dies eine unbefugte Nutzung dieser ihm nur zu dienstlichen Zwecken eingeräumten Zugriffsbefugnis dar. Gewissheit über eine mögliche Einstellung seiner Daten in INPOL wäre ohne Probleme durch einen Auskunftsantrag nach § 47 PAG möglich gewesen. Da ein unbefugter Zugriff auf polizeiliche Daten den Tatbestand des § 43 Abs. 1 Nr. 1 ThürDSG darstellt, hat die Polizeidirektion Gotha die festgestellten unbefugten bzw. nicht nachgewiesenen befugten Fälle von Abrufen an die Staatsanwaltschaft Erfurt zur weiteren Prüfung übergeben. Dass darunter auch die Selbstabrufe des betroffenen Polizeibeamten sind, stellt keine Benachteiligung des Beschwerdeführers nach § 11 Abs. 2 ThürDSG dar, weil der Nachteil einer möglichen strafrechtlichen Ahndung nicht unmittelbar durch die Beschwerde beim TLfD ausgelöst wurde, sondern eine

Folge der Kontrolltätigkeit darstellt und zudem nicht nur die Selbstabfragen sondern alle unbefugten Abfragen verfolgt wurden.

Beamte haben eine strikte Trennung von dienstlichen und privaten Interessen bei der Dienstausübung einzuhalten. Die aus den ermittelten Einzelfällen gezogenen straf- und disziplinarrechtlichen Konsequenzen sind daher von besonderer Bedeutung, um eine abschreckende Wirkung für die Zukunft zu entfalten. Nach wie vor verbesserungswürdig bleibt jedoch der Umfang der Protokollierung, insbesondere zum Grund der Abfrage.

7.6 Erweitertes Verfahren in der Zentralen Bußgeldstelle geprüft

Bereits vor einiger Zeit hatte der TLfD die technischen und organisatorischen Maßnahmen in der Zentralen Bußgeldstelle (ZBS) geprüft (vgl. 6. TB, 7.10). Nach einer gewissen Zeit sollten die organisatorischen Regelungen einer stichprobenartigen Überprüfung unterzogen werden. Anlass dafür bot im Jahr 2011 die Erweiterung des bisherigen Fachverfahrens um ein Modul zur dezentralen Erfassung von Ordnungswidrigkeiten in den Polizeidienststellen des Landes sowie deren Zugriff auf zentral gespeicherte Daten über eingezogene Führerscheine. Bei einem Kontrollbesuch waren keine grundlegenden Mängel festzustellen. So lag insbesondere ein verfahrensspezifisches Sicherheitskonzept vor. Lediglich die konkreten Regelungen zum Umgang mit dem Administratorenpasswort, das in einem Safe aufbewahrt wird, waren verbesserungsbedürftig. So hat der TLfD eine klare Regelung gefordert, welcher Personenkreis auf das Passwort zugreifen kann und dass eine Verfahrensweise festzulegen ist, wonach der Zugriff auf das hinterlegte Administratorenpasswort nur durch Zusammenwirken von zwei Personen im Vier-Augen-Prinzip erfolgen darf und zu dokumentieren ist. Dem ist die ZBS zwischenzeitlich nachgekommen. Auch bei den neuen Funktionalitäten des Fachverfahrens gab es Hinweise des TLfD zur Verbesserung des Datenschutzes. Hintergrund der Erweiterung war der Verwaltungsaufwand durch die Eingabe von Erfassungsbelegen zu Ordnungswidrigkeiten in das System, die zuvor von den Polizeidienststellen schriftlich der ZBS übermittelt worden waren. Bislang musste diese Arbeit bei der Polizei zweimal erfolgen: Einmal in der jeweiligen Polizeidienststelle und ein zweites Mal in der ZBS. Mit der Erweite-

rung wurden über das polizeiinterne Netz Schnittstellen zu dem zentralen Verfahren eingerichtet, über die solche Erfassungsbelege direkt in das System der ZBS eingegeben werden können. Dabei ist sichergestellt, dass nach der Eingabe kein Zugriff mehr auf die eingegebenen Daten möglich ist und die weitere Bearbeitung ausschließlich durch die ZBS erfolgt. Eine weitere Funktion betrifft die Möglichkeit, aus dem zentralen Bestand nach verhängten Fahrverboten im Zusammenhang mit Verkehrsordnungswidrigkeitenverfahren zu recherchieren. Damit handelt es sich nicht nur um ein Datenübermittlungsverfahren, sondern um ein automatisiertes Abrufverfahren, bei dem nach den Vorschriften der StPO (§ 49 c Abs. 1 OWiG i. V. m. § 488 Abs. 3 Satz 3 StPO) die ZBS sicherzustellen hat, dass zumindest durch geeignete Stichprobenverfahren geprüft werden kann, ob die Abrufe jeweils auch rechtmäßig erfolgt sind. Das Wissen, ob jemand seine Fahrerlaubnis abgeben musste, kann auch für einen Polizeibeamten privat von Interesse sein (siehe dazu 7.5). Deshalb müssen auch Regelungen zur Protokollierung von Zugriffen durch Bedienstete und deren Auswertung getroffen sein. Solche Regelungen lagen jedoch nicht ausdrücklich vor, wurden jedoch nach Hinweis durch den TLfD von der ZBS aufgenommen.

Auch bei der Erweiterung von Verfahren ist immer zu prüfen, ob die getroffenen technischen und organisatorischen Maßnahmen noch ausreichend sind.

7.7 Aktenzeichen darf nicht ins Adressfeld

Nach Veränderung eines Fachverfahrens hatte die ZBS bei der automationsgestützten Erstellung von Anschreiben neben der Anschrift regelmäßig auch das Aktenzeichen in das Adressfeld von Sichtumschlägen aufgenommen. Das hat zu mehreren Beschwerden beim TLfD geführt, da die Betroffenen darin eine unrechtmäßige Offenbarung ihrer persönlichen Daten an Dritte sahen. Zum Teil wurde zudem noch der Umstand kritisiert, dass im Sichtfenster auch die Absenderangabe „Thüringer Polizei, Zentrale Bußgeldstelle 06553 Artern“ aufgedruckt war. Damit könnten Personen aus dem Umfeld der Betroffenen unschwer auf den Inhalt der Sendungen schließen. Die ZBS hatte zur Begründung für diese Vorgehensweise darauf hingewiesen, dass bei förmlichen Zustellungen ohnehin das

Aktenzeichen auf der Außenseite der Sendung anzubringen sei und in den übrigen Fällen die Anordnung im Sichtfenster bei häufig vorkommenden Rücksendungen eine Zuordnung zu einem Vorgang schnell und zielsicher erlaube. Zudem sei eine Umprogrammierung sämtlicher etwa 200 verwendeter Vorlagen sehr aufwändig. Ein Datenschutzproblem bestehe dabei schon deswegen nicht, weil es sich bei dem Aktenzeichen um kein personenbezogenes Datum handele. Dies wurde vom TLfD anders gesehen. Bei dem Aufdruck des Aktenzeichens auf Briefsendungen ist von einer Übermittlung von personenbezogenen Daten i. S. d. § 3 Abs. 1 ThürDSG zu einer bestimmaren natürlichen Person an den Postdienstleister auszugehen. Eine Rechtsgrundlage hierfür ist nur bei förmlichen Zustellungen von Bußgeldbescheiden gegeben, da hier die Angabe einer Geschäftsnummer auf der Briefsendung vorgeschrieben ist. Eine Rechtsgrundlage zur Übermittlung dieses Datums an den Postdienstleister bei allen übrigen Sendungen gibt es nicht, da es bereits an einer Erforderlichkeit zur Erfüllung der Aufgaben der in der Zuständigkeit der Zentralen Bußgeldstelle i. S. d. § 22 Abs. 1 Nr. 1 ThürDSG fehlt. Von einer Datenübermittlung an Nachbarn oder Familienmitglieder, wie von den Beschwerdeführern angenommen, kann man hier aber nicht ausgehen, weil die Verantwortung der ZBS als Absender für dieses personenbezogene Datum mit der Übergabe an den Postdienstleister endet. Hierfür muss der Empfänger in seinem Einflussbereich Sorge tragen, wenn er Postsendungen und deren Absender in seinem persönlichen Umfeld Dritten nicht zur Kenntnis gelangen lassen möchte. Das kann z. B. dadurch geschehen, dass der Briefkasten immer selbst geleert und auch Nachbarn kein Briefkastenschlüssel überlassen wird. Bei dem von der ZBS verwendeten Aktenzeichen handelt es sich aber um kein sogenanntes sprechendes Aktenzeichen, aus dem bereits bestimmte Rückschlüsse auf einen möglichen Inhalt der Sendung gezogen werden kann. Allerdings besteht die Gefahr, dass durch die Kenntnis des Aktenzeichens bei telefonischen Anfragen weitere Informationen des Betroffenen erschlichen werden könnten. Daher müssen grundsätzlich nach § 9 ThürDSG technische und organisatorische Maßnahmen ergriffen werden, um die Ausführungen der Bestimmungen des ThürDSG zu gewährleisten. Das ist dadurch zu erreichen, dass künftig auf die Angabe des Aktenzeichens im Klartext zugunsten eines Barcodes verzichtet wird. Mit der ZBS wurde eine Einigung dahingehend erzielt, dass mittelfristig die Entfernung des Aktenzeichens aus dem

Sichtfenster erfolgen wird. Zwischenzeitlich hat die ZBS ihre Dienstanweisungen dahingehend ergänzt, dass bei telefonischen Auskünften eine eindeutige Identifizierung nicht nur anhand der auf dem Umschlag aufgedruckten Daten erfolgen darf, sondern darüber hinausgehende identifizierende Daten abgefragt werden müssen, um sich Gewissheit von der Identität des Betroffenen zu verschaffen. Dadurch soll der Gefahr begegnet werden, dass Dritte sich Informationen zu den laufenden Bußgeldverfahren über das Aktenzeichen erschleichen können. Gegen die Angabe des Absenders „Thüringer Polizei - Zentrale Bußgeldstelle“ bestehen nicht nur keine Bedenken, sondern sie ist bereits deshalb erforderlich, damit Rücksendungen an den korrekten Absender erfolgen können und die Sendungen nicht von Stellen geöffnet werden müssen, die überhaupt nicht der Absender waren.

Nach einer Übergangszeit wird die ZBS das Aktenzeichen wieder aus Adressfeldern von Briefsendungen entfernen. Damit wird auch eine größere Akzeptanz bei den Betroffenen hergestellt. Allerdings müssen sie in ihrem persönlichen Umfeld selbst für die gewünschte Vertraulichkeit sorgen.

8 Verfassungsschutz

8.1 Evaluierung und Verlängerung der Terrorismusbekämpfungsgesetze

In den letzten zehn Jahren sind nach den terroristischen Anschlägen vom 11. September 2001 eine große Zahl von Sicherheitsgesetzen in Bund und Ländern mit dem Ziel verschärft worden, den internationalen Terrorismus wirksam zu bekämpfen. Dabei wurden auch eine Vielzahl von Befugnissen zum Eingriff in die Privatsphäre der Bürgerinnen und Bürger geschaffen, ohne die fortbestehende Notwendigkeit und die möglichen Auswirkungen solcher Maßnahmen einer fundierten Überprüfung zu unterziehen. Da diese Änderungen meist unter großem Zeitdruck erfolgten, wurden einige dieser gesetzlichen Eingriffsbefugnisse einer Befristung unterworfen. Wiederum ein Teil der befristeten Normen sind mit einer Evaluierungsklausel versehen worden. Ein Beispiel hierfür war das TerrorBekämpfG vom 9. Januar 2002, mit dem das BfV u. a. die Befugnis erhielt, bei Banken Auskünfte zu Konten und deren Inhaber, bei Postunternehmen Auskünfte zu Namen, Anschriften, Postfächern und sonstigen Umständen des Postverkehrs sowie bei Telekommunikations- und Internetunternehmen Auskünfte über Verbindungs- und Nutzungsdaten einzuholen. Artikel 22 TerrorBekämpfG sah eine Befristung für fünf Jahre vor und ordnete lediglich an, dass „die Neuregelungen vor Ablauf der Befristung zu evaluieren sind“. Eine unabhängige Evaluation erfolgte im Jahr 2006 nicht, weil die Prüfung der Erforderlichkeit einer Verlängerung des Gesetzespakets durch die Bundesregierung selbst erfolgte. Dabei war es nicht verwunderlich, dass nicht nur die bisherigen Regeln weitergelten sollten, sondern Befugnisse, die bislang nur für das Bundesamt für Verfassungsschutz galten, auch auf den Bundesnachrichtendienst und den Militärischen Abschirmdienst ausgeweitet worden sind. Mit einer verbesserten Evaluierungsklausel in Artikel 11 Terrorismusbekämpfungsergänzungsgesetz (TerrorBekämpfErgG) vom 5. Januar 2007 sollte auch der von den Datenschutzbeauftragten des Bundes und der Länder erhobenen Forderung nach einer unabhängigen Evaluierung auf wissenschaftlicher Grundlage Rechnung getragen werden. So sollte die Evaluierung unter Einbeziehung eines (!) wissenschaftlichen Sachverständigen erfolgen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird. Kurz vor Ablauf der weiteren Verlän-

gerung des Gesetzes Anfang 2012 legte die Bundesregierung im Sommer 2011 einen Gesetzentwurf zur Änderung des Bundesverfassungsschutzgesetzes vor, der ein Auslaufen derjenigen Befugnisse des Verfassungsschutzes vorsah, von denen seit deren Einführung kein Gebrauch gemacht worden ist. Dies betraf u. a. die Auskünfte von Postunternehmen zu Bestandsdaten oder Umständen des Postverkehrs. Im Übrigen sollen aber die sonstigen Befugnisse für weitere fünf Jahre fortgelten. Veränderungen gab es auch bei der parlamentarischen Kontrolle und der Möglichkeit nicht nur bei den Fluggesellschaften, sondern auch bei den Betreibern von Buchungssystemen Daten abzufragen. Die erweiterte Evaluierungsklausel in Artikel 9 des Gesetzentwurfs scheint die mehrfach von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Entschließungen (Anlagen 5 und 23) geforderte wissenschaftlich fundierte Evaluierung zumindest zum Teil aufgegriffen zu haben. Dort ist jetzt vorgesehen, dass unter Mitwirkung eines oder mehrerer wissenschaftlicher Sachverständiger, die im Einvernehmen mit dem Deutschen Bundestag bestellt werden, auch die Häufigkeit und die Auswirkungen der mit den Eingriffsbefugnissen verbundenen Grundrechtseingriffe einzubeziehen sind. Diese Grundrechtseingriffe sind dann in Beziehung zu setzen zu der anhand von Tatsachen darzustellenden Wirksamkeit der Normen zum Zweck der Terrorismusbekämpfung.

Im Thüringer Verfassungsschutzgesetz (ThürVerfSchG) wurden die erweiterten Eingriffsbefugnisse des Bundesamtes für Verfassungsschutz seit dem Jahr 2001 jeweils durch direkte Verweise auf das Bundesverfassungsschutzgesetz (BVerfSchG) in das Landesrecht übernommen. Zwar erfolgte jeweils eine Befristung für fünf Jahre. Eine Evaluierung war jedoch bislang nicht vorgesehen. Entsprechende Forderungen des TLfD (7. TB, 8.2) hat die Landesregierung mit dem Argument zurückgewiesen, dass es sich bei diesen Befugnissen lediglich um die verwaltungsmäßige Umsetzung des Bundesrechts im Landesrecht handle. Da jedoch der Landesgesetzgeber insoweit autonom Recht setzt, könnte er sehr wohl die Auswirkungen dieser Eingriffsbefugnisse im Bereich des Landes einer unabhängigen Evaluierung unterziehen und dann entscheiden, ob er sich weiterhin den im Bundesverfassungsschutzgesetz enthaltenen Eingriffsbefugnissen durch eine Gesetzesverweisung anschließt oder davon abweichende Regelungen trifft. Denkbar ist zudem, dass die Erkenntnisse

aus einer solchen Evaluierung auf Landesebene auch in die Evaluierung nach Artikel 9 des am 10. Januar 2011 in Kraft getretenen Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes einfließen könnten. Die Landesregierung hat im Herbst 2011, kurz vor Ablauf der Befristung des ThürVerfSchG und einiger anderer Gesetze, den Entwurf eines Gesetzes zur Änderung sicherheits- und melderechtlicher Vorschriften vorgelegt, mit dem das Thüringer Sicherheitsüberprüfungsgesetz, das Thüringer Ausführungsgesetz zum G-10-Gesetz sowie das ThürMeldeG entfristet werden sollen. Das ThürVerfSchG soll im Jahr 2012 an die o. g. Änderungen des BVerfSchG angepasst werden. Deshalb hat der Landtag einer nochmaligen Befristung für ein Jahr bis zum 31. Dezember 2012 zugestimmt. In einer schriftlichen Anhörung des Innenausschusses hat der TLfD darauf hingewiesen, dass die Zeit bis zum Ende der Befristung für eine Evaluierung der Befugnisse durch eine unabhängige Stelle genutzt werden sollte. Der Anregung, eine solche Evaluierungspflicht in den Gesetzentwurf aufzunehmen, ist der Landtag nicht gefolgt.

Es bleibt zu hoffen, dass in den jeweils anstehenden Änderungen der Befugnisse der Verfassungsschutzbehörden auf Bundes- und Landesebene zur Terrorismusbekämpfung endlich eine wissenschaftliche Evaluierung durch eine unabhängige Stelle erfolgt.

8.2 NADIS neu – Probleme mit der Volltextsuche

Das nachrichtendienstliche Informationssystem (NADIS) wird technisch vom BfV betrieben und steht als Verbunddatei den Verfassungsschutzämtern des Bundes und der Länder bereits seit vielen Jahren zum Austausch von Informationen entsprechend den gesetzlichen Grundlagen zur Verfügung. Nun soll dieses System auf den technisch neuesten Stand gebracht werden. Eine unter Federführung des BfV tätige Projektgruppe der Verfassungsschutzämter bereitet diese Neuausrichtung vor. Wie so oft führen neue technische Möglichkeiten im Bereich der Verarbeitung personenbezogener Daten zu zusätzlichen Gefährdungen für das Persönlichkeitsrecht der Betroffenen, auf die durch technische und organisatorische Maßnahmen oder auch durch Anpassung rechtlicher Regelungen reagiert werden muss. Nach der geltenden Rechtslage ist es nicht zulässig, dass in NADIS ein vollständiges elektronisches Abbild der personenbezogenen

nen Informationen zum unbeschränkten Abruf für alle angeschlossenen Verfassungsschutzämter bereitgestellt wird. Grund hierfür sind die häufig sehr sensiblen, aber auch vielfach nicht gesicherten Erkenntnisse, die zudem auch zufällig mitbetroffene Personen zum Gegenstand haben können. Deshalb enthält der Großteil der gespeicherten Datensätze in strukturierter Form nur Daten, die zur Identifizierung einer Person führen und die jeweils eingebende Stelle benennen. Führt eine Recherche zum Treffer, so werden die weitergehenden Informationen direkt zwischen den beteiligten Behörden unter Beachtung der gesetzlichen Vorschriften ausgetauscht.

Mit NADIS WN (= Wissensnetz) sollen jedoch nicht nur strukturierte Daten, sondern auch unstrukturierte Textdateien zum Abruf bereitgestellt werden. Das vereinfacht die Arbeit der beteiligten Behörden, weil das entsprechende Ursprungsdokument direkt aus dem System abgerufen werden kann, ohne dass eine weitere Kontaktaufnahme mit der jeweiligen Behörde nötig ist. Daneben entsteht durch die Möglichkeit, in dem strukturierten Gesamtdatenbestand mit Suchwerkzeugen sämtliche Dateien z. B. nach Namen oder sonstigen personenbezogenen Merkmalen zu durchsuchen, eine neue Qualität der Datenverarbeitung, die mit einem sogenannten Data-Warehouse oder einer Internetsuchmaschine verglichen werden könnte, wobei die Suchberechtigten auf die Mitarbeiter der Verfassungsschutzämter entsprechend den jeweiligen Zugriffsrechten beschränkt werden. Auf die besonderen Risiken, die von einer Volltextrecherche in Datenbeständen der Sicherheitsbehörden ausgehen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 10) hingewiesen und die Bundesregierung und die Landesregierungen aufgefordert, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten. Besonders problematisch ist hierbei der Umstand, dass durch solche Volltextrecherchen auch nach solchen Personen gesucht werden kann, die überhaupt nicht Zielpersonen der Sicherheitsbehörden sind, sondern nur zufällig als Beteiligte oder Familienangehörige in den Texten erwähnt sein können. Nach Kritik durch die Datenschutzbeauftragten des Bundes und der Länder, die von Zeit zu Zeit über den Entwicklungsstand im Arbeitskreis Sicherheit durch das BfV informiert wurden, ist die Konzeption dahingehend geändert worden, dass keine Ursprungsdokumente im System gespeichert werden, in denen Unbeteiligte

genannt sind. Zudem soll die Volltextrecherche in Ursprungsdokumenten nur einem relativ kleinen Kreis innerhalb der Verfassungsschutzbehörden möglich sein. Eine ursprünglich geplante Inbetriebnahme im Jahr 2011 wird nun wohl erst im Jahr 2012 erfolgen.

Die Einhaltung der verfassungsrechtlichen Grenzen bei der Volltextrecherche im NADIS-WN wird auch nach Einführung des neuen Systems von den Datenschutzbeauftragten überprüft werden.

8.3 Hosting der Amtsdatei des TLfV durch das BfV nur mit ausreichender Kontrolle

In einem gewissen Zusammenhang mit dem geschilderten System NADIS-neu (s. o. 8.2) steht auch die Möglichkeit, die das BfV den Landesämtern für Verfassungsschutz anbietet, in seinem generischen Dateisystem die Amtsdateien des jeweiligen Landesamtes technisch zu betreiben. Das hat den Vorteil v. a. für kleinere Ämter, dass sie selbst keine eigene Technik hierfür vorzuhalten brauchen. Der Vorteil für das BfV und den nachrichtendienstlichen Verbund liegt darin, dass die Struktur der Amtsdateien sehr stark an das System NADIS WN angepasst ist, und so eine Überführung von Daten nach NADIS sehr einfach erfolgen kann, wenn die rechtlichen Voraussetzungen dafür vorliegen. Hiergegen ist aus datenschutzrechtlicher Sicht nichts einzuwenden. Im Jahr 2010 hat sich auch das TLfV entschieden, von dem Angebot des BfV Gebrauch zu machen. Hierzu hat es mit dem BfV eine Verwaltungsvereinbarung abgeschlossen, in der u. a. die Verantwortungsteilung für den Betrieb der Datei festgelegt wird. Danach wird die Datei vom BfV technisch betrieben. Das TLfV trägt demgegenüber die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung, die Aktualität der Daten und die Auskunftserteilung an die Betroffenen. Vom TLfD wurde hier in Frage gestellt, ob es sich bei diesem technischen Betrieb lediglich um eine Amtshilfe auf der Grundlage von § 1 Abs. 3 BVerfSchG handelt. Nach dieser Vorschrift besteht die Zusammenarbeit der Verfassungsschutzämter des Bundes und der Länder auch in gegenseitiger Unterstützung und Hilfeleistung. Daraus leitet das TLfV eine Befugnis des BfV zum Hosting seiner Amtsdatei ab. Allerdings gehen dabei das TLfV und der TLfD von einer unterschiedlichen Einordnung dieser Dienstleistung aus. Das TLfV sieht darin lediglich eine technische Unterstützungsleistung, bei der keine personenbezo-

genen Daten verarbeitet werden. Allerdings wird dann doch die Notwendigkeit gesehen, dass auch technische Kontrollmaßnahmen zum Datenschutz sichergestellt werden müssen. So soll das BfV die technischen Maßnahmen zur Datensicherheit treffen und auf Anforderung des TLfV Protokolle von Datenzugriffen zur Datenschutzkontrolle zur Verfügung stellen. Die Datenschutzkontrolle vor Ort soll jedoch ausschließlich durch den BfDI erfolgen. Das sieht der TLfD etwas anders: Auch wenn die Daten nicht vom BfV planmäßig verarbeitet oder genutzt werden sollen, kann das BfV doch auf den Datenbestand einwirken und diesen z. B. löschen, auch wenn das nicht zulässig sein sollte. Zudem besitzt auch der Systemadministrator des BfV die Möglichkeit, sich einen temporären Benutzer einzurichten und damit Zugang zu den Daten des TLfV zu erlangen. Deshalb handelt es sich bei dem Hosting nach Auffassung des TLfD um eine Verarbeitung personenbezogener Daten durch das BfV. Eine Übermittlung dieser Daten ist nach dem ThürVerfSchG und dem BVerfSchG jedenfalls nicht zulässig, soweit die Daten nicht in den Bestand der Verbunddatei NADIS gehören. Somit bliebe als Rechtsgrundlage allenfalls eine Datenverarbeitung im Auftrag nach § 8 ThürDSG. Hierzu argumentiert das TLfV, dass § 1 Abs. 3 BVerfSchG die Anwendbarkeit des § 8 ThürDSG als Spezialgesetz verdrängen würde. Eine solche Sichtweise verkennt den Grundsatz, dass sich aus Aufgabennormen keine Eingriffsbefugnisse ableiten lassen. Aus der Pflicht zur gegenseitigen Unterstützung lässt sich keine Befugnis zur Datenverarbeitung ableiten. Der eigentliche Grund, weshalb die Anwendbarkeit der Vorschriften für eine Datenverarbeitung im Auftrag abgelehnt wird, sind die weiteren Konsequenzen für den Auftragnehmer, hier das BfV. Dieses müsste sich vertraglich der Kontrolle der Datenverarbeitung durch das TLfV unterwerfen, was kategorisch abgelehnt wird. So ist nun die Situation entstanden, dass das TLfV das Hosting mit dem BfV beenden müsste, wenn es dieses als Auftragsdatenverarbeitung einordnet. Die Datenschutzbeauftragten des Bundes und der Länder sind sich einig, dass allenfalls eine Einordnung als Auftragsdatenverarbeitung in Betracht kommt. Eine Lösung des Problems könnte nur dadurch geschaffen werden, dass in einer gesetzlichen Regelung im BVerfSchG das Hosting ausdrücklich zugelassen wird, wobei jedoch auch eindeutig festgelegt werden müsste, wer die Datenschutzkontrolle in welchem Bereich übernehmen soll, da keine Kontrolllücken entstehen dürfen.

Es sollte eine gesetzliche Regelung des Hostings der Amtsdateien durch das BfV im BVerfSchG aufgenommen werden, bei der die Datenschutzkontrolle eindeutig geregelt ist.

9 Finanzwesen

9.1 Haushaltsmanagementsystem (HAMASYS)

Im 8. Tätigkeitsbericht (9.2) hatte der TLfD über verschiedene Datenschutzprobleme bei der Anwendung des Verfahrens HAMASYS berichtet. Wie durch das TFM zugesagt, ist mit der Überarbeitung des Verfahrens nunmehr auch eine Kenntnisnahme von bereits zuvor gespeicherten personenbezogenen Daten zu konkreten Zahlungsvorgängen durch Unberechtigte ausgeschlossen. Nicht ausgeräumt wurden bislang jedoch die datenschutzrechtlichen Bedenken hinsichtlich der Zugriffsrechte auf die Partnerdaten im Verfahren HAMASYS. Das hat folgenden Hintergrund:

Die im Verfahren verwendeten Partnerdaten enthalten personenbezogene Informationen (Name, Adresse, Bankverbindung und Steuer-Nummer) von Zahlungspflichtigen und Zahlungsempfängern. Nur für Datensätze, die eine Zahlung im Rahmen von Trennungsgeld, Reisekosten oder Beihilfe vorsehen, ist die Vertraulichkeit dadurch gewährleistet, dass nur die für den jeweiligen Zahlungsvorgang berechtigten Stellen Zugriff besitzen. Alle anderen Partnerdaten stehen nach ihrer Erfassung – es handelt sich hierbei um mehr als 200.000 Datensätze – standardmäßig ca. 3.840 Mitarbeitern aller Landesbehörden, die das System nutzen, zur Verfügung.

Nach Auffassung des TLfD werden bei der Nutzung von HAMASYS Vorschriften über den Datenschutz verletzt, weil die o. g. personenbezogenen Daten ohne geeignete Rechtsgrundlage und ohne Einwilligung der Betroffenen auch Stellen ohne jegliche Zuständigkeit standardmäßig zur Verfügung gestellt werden. Darüber hinaus stellt die Einräumung von Zugriffsberechtigungen für alle HAMASYS nutzenden Dienststellen ein automatisiertes Abrufverfahren nach § 7 ThürDSG dar, das wegen der entgegenstehenden schutzwürdigen Interessen der Betroffenen nicht als angemessen und mangels Einwilligung der Betroffenen als unzulässig anzusehen ist. Niemand, der mit einer Behörde haushaltsrelevante Vorgänge abwickelt, muss auch annehmen, dass neben den zuständigen Mitarbeitern auch Bedienstete anderer Behörden auf seine Adress- und Bankverbindungsdaten zugreifen können.

Nach § 4 Abs. 1 ThürDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hat. Mangels geeigneter Rechtsvorschriften – auch die spezialgesetzlichen Vorschriften etwa der Thüringer Landeshaushaltsordnung bzw. des Haushaltsgrundsätzegesetzes helfen hier nicht weiter – kommt eine Speicherung und Bereitstellung der Partnerdaten für alle an HAMASYS beteiligten Dienststellen nur in Betracht, wenn der Betroffene hierin eingewilligt hat. Vor einer Einwilligung hat die verantwortliche Stelle den Betroffenen über die Datenspeicherung und deren Umfang zu unterrichten. Die Einwilligung ist dabei nachvollziehbar zu gestalten. Trotz der bereits im 8. TB veröffentlichten Problematik wurde bei Kontrollen festgestellt, dass die mit ihren Partnerdaten erfassten Personen bisher nicht darüber in Kenntnis gesetzt wurden, dass sämtliche an HAMASYS beteiligte Behörden über die Möglichkeit verfügen, die personenbezogenen Partnerdaten abzurufen.

Besonders schwer wiegt der festgestellte Gesetzesverstoß seitens des TFM, weil ihm die Betreuung des Verfahrens für die gesamte Landesverwaltung obliegt und es selbst jahrelang diese unzulässigen Datenübermittlungen durchgeführt hat. Der TLfD hatte das TFM gebeten, umgehend eine datenschutzkonforme Gestaltung des Verfahrens zu veranlassen. Hierbei wurde folgende datenschutzfreundliche Verfahrensweise vorgeschlagen:

Bei der erstmaligen Erfassung eines Zahlungspartners sind dessen Daten standardmäßig nur den berechtigten Mitarbeitern der unmittelbar mit dem Zahlungsvorgang befassten Behörden zur Verfügung zu stellen. Zugleich kann dem Betroffenen bei Bedarf eine Einwilligung zur Veröffentlichung dieser Daten für alle beteiligten Behörden angeboten werden. Diese Maßnahme sollte für alle angeschlossenen Behörden einheitlich umgesetzt werden. Die bereits im System befindlichen Partner könnten durch die jeweils zuständigen Stellen sukzessive um eine nachträgliche Einwilligung gebeten werden. Dass dieser Vorschlag mit angemessenem Aufwand realisiert werden kann, zeigt sich daran, dass bereits derzeit bei der Erfassung durch die zuständige Behörde der Zugriff auf Partnerdaten im Falle von Trennungsgeld, Reisekosten und Beihilfe durch Aktivierung eines speziellen Schutzrechtes auf die berechtigten Dienststellen und

Mitarbeiter beschränkt werden kann. Da das TFM der Aufforderung des TLfD nicht Folge leistete, hat der TLfD das Verfahren HAMASYS gemäß § 39 Abs. 1 ThürDSG beanstandet. Nachfolgend kamen das TFM und der TLfD überein, dass künftig bei Neuaufnahmen von Partnern in HAMASYS durch die Mittel bewirtschaftenden Stellen eine Einverständniserklärung zu einer Verwendung der Adress- und Kontodaten im Verfahren HAMASYS einzuholen ist. Das TFM sagte zu, ein Formular für eine solche Einverständniserklärung zu entwickeln und allen Ressorts zur Verfügung zu stellen, wobei ausdrücklich auf die datenschutzrechtliche Problematik hingewiesen werden soll. Im Falle der nicht erteilten Einwilligung soll künftig gewährleistet sein, dass der Zugriff auf die Daten nur durch die unmittelbar am Zahlungsvorgang beteiligten Stellen möglich ist.

Eine Datenübermittlung ist nur dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder soweit der Betroffene hierin eingewilligt hat. Diese Zulässigkeitsvoraussetzung gilt auch für automatisierte Abrufverfahren im Rahmen der Landesverwaltung.

9.2 Was darf das Finanzamt bei der Sachverhaltsermittlung?

Durch Beschwerden von Bürgern wird immer wieder die Frage aufgeworfen, welche persönlichen Daten die Finanzämter zur Sachverhaltsermittlung erheben dürfen. So wurde in einem Fall die Arbeitsweise des Finanzamts Ilmenau hinterfragt, im Rahmen einer Umsatzsteuer-Nachschaу den Arbeitsraum der geschäftlich genutzten Wohnung zu fotografieren. Hier gilt, dass die Möglichkeit einer Bilddokumentation insbesondere bei unklaren Sachverhalten genutzt werden kann, wenn es auf die zweifelsfreie Dokumentation der vorgefundenen Verhältnisse ankommt. Rechtsgrundlage für diese Dokumentation sind § 98 und § 99 AO. Dabei dürfen Wohnräume grundsätzlich nicht gegen den Willen des Inhabers betreten werden (§ 99 Abs. 1 Satz 2 AO). Gleiches gilt nach Auffassung des TLfD auch für fotografische Dokumentationen anlässlich eines solchen Besuches. Diese Voraussetzungen waren im konkreten Fall erfüllt, da es der Beschwerdeführer gestattet hatte, die vorgefundenen Örtlichkeiten zu fotografieren und die Fotos nach der Anfertigung des Aktenvermerks wieder gelöscht worden waren.

Will ein Steuerpflichtiger geschäftlich bedingte Bewirtungskosten in seiner Einkommenssteuererklärung als Betriebsausgaben steuermindernd geltend machen, dann tritt häufig die Frage auf, wie detailliert er diese Kosten nachweisen muss. Um glaubhaft zu machen, dass er potentielle Kunden aus geschäftlichem Anlass bewirtet hat, ist es vorgeschrieben (§ 4 Abs. 5 Satz 1 Nr. 2 EStG), dem Finanzamt den Anlass und die Teilnehmer der Bewirtung schriftlich vorzulegen. Fraglich ist, ob neben den Namen der Teilnehmer auch deren Anschriften vom Finanzamt verlangt werden können. Rechtsprechung und die herrschende Meinung in der Literatur stufen diese Angaben als im Regelfall nicht erforderlich ein. Sofern sich allerdings im Einzelfall Zweifel an den Angaben des Steuerpflichtigen ergeben sollten, können die Adressen der Teilnehmer nachgefordert werden. So hatte das Finanzamt Erfurt von einem Beschwerdeführer zunächst die Anschriften der Teilnehmer einer Bewirtung verlangt. Für diese Aufforderung sah der Beschwerdeführer keinen hinreichenden Grund. Die daraufhin erfolgte Einzelfallüberprüfung ergab, dass von einer Nachforderung der Anschriften der bewirteten Gäste Abstand genommen wurde.

Im Rahmen einer Umsatzsteuer-Nachschau sind Fotos der hierfür relevanten Örtlichkeiten nur mit Zustimmung des Betroffenen zulässig. Nach erfolgter Auswertung sind diese Fotos unverzüglich zu löschen.

Anschriften von bewirteten Personen sind zur Geltendmachung von Betriebsausgaben nur ausnahmsweise gegenüber den Finanzbehörden anzugeben.

9.3 Automatische Anzeige des Kontostands nach Verfügungen am Geldautomaten

Eine Beschwerde betraf die Diskretion an Geldautomaten der Kreissparkasse Nordhausen. Zuvor hatte die Sparkasse veranlasst, dass im Anschluss an Bargeldverfügungen am Bildschirm der Geldautomaten auch der Kontostand automatisch angezeigt wird, um den Kunden separate Kontostandsabfragen bzw. Kontoausdrucke zu ersparen. Wie der Beschwerdeführer mitteilte, müsse man am Geldautomaten nunmehr noch zusätzlich darauf achten, dass der Kontostand vertraulich bleibt. In diesem Zusammenhang sei festzustellen, dass die Hinweise auf die Diskretionszone vor den Geldautomaten in ver-

schiedenen Einkaufszentren mangelhaft seien. Auf Anregung des TLfD wurden inzwischen in den Selbstbedienungsfilialen der Sparkasse Fußbodenaufkleber angebracht, die deutlich wahrnehmbar auf die gebotene Einhaltung der Diskretionszonen vor den Geldautomaten hinweisen und einige Geldautomaten mit erweiterten Sichtblenden ausgestattet. Diese Maßnahmen sind geeignet, ein höheres Maß an Vertraulichkeit bei der Nutzung der Geldautomaten zu gewährleisten. Unter der Voraussetzung, dass diese Maßnahmen sachgerecht umgesetzt werden, ist es als datenschutzrechtlich vertretbar anzusehen, die automatische Anzeige des Kontostandes im unteren Teil des Bildschirms des Geldautomaten beizubehalten.

Hinweisschilder und Sichtblenden sind unter bestimmten Umständen als geeignete Mittel zum Schutz sensibler personenbezogener Daten anzusehen. Günstiger ist es jedoch, von vorneherein auf eine automatische Anzeige sensibler Daten zu verzichten.

10 Justiz

10.1 Vorratsdatenspeicherung – quo vadis?

Wie im letzten Tätigkeitsbericht unter 4.1 dargestellt, hatte das Bundesverfassungsgericht die damalige Umsetzung der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung im TKG gestoppt, eine Vorratsdatenspeicherung jedoch unter engen Voraussetzungen als verfassungsrechtlich zulässig angesehen. Daher ist es in der Bundesrepublik Deutschland weiterhin möglich, die Richtlinie mit einem neuen Gesetz umzusetzen. Hierzu ist es bislang nicht gekommen. Das Bundesministerium der Justiz hat Anfang 2011 ein Eckpunktepapier „Zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdaten und Auskünften im Internet“ veröffentlicht. Ein konkreter Gesetzentwurf zur Umsetzung ist jedoch nicht bekannt. So bleibt weiterhin abzuwarten, ob und in welcher Art und Weise eine Vorratsdatenspeicherung ermöglicht wird. Zwischenzeitlich hat die Europäische Kommission ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, mit dem die Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung gefordert wird. Aus datenschutzrechtlicher Sicht bestehen nach wie vor Vorbehalte gegenüber einer langfristigen Speicherung von Telekommunikationsverkehrsdaten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 17./18. März 2010 („Keine Vorratsdatenspeicherung“ - Anlage 3) die grundsätzliche Ablehnung einer Vorratsdatenspeicherung geäußert.

Im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen ist der Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen zu größerer Zurückhaltung aufgerufen.

10.2 Keine Quellen-TKÜ ohne gesetzliche Grundlage in der Strafprozessordnung

Die Überwachung der Telekommunikation kann bekanntlich bei Vorliegen der Voraussetzungen grundsätzlich auf der Grundlage von § 100 a, b StPO erfolgen. Wollen Strafverfolgungsbehörden verschlüsselte Internettelefonie oder E-Mails überwachen und aufzeichnen (sogenannte Quellen-Telekommunikationsüberwachung,

Quellen-TKÜ) muss hierzu auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet. Die Technik entspricht dabei der Online-Durchsuchung („Trojaner“), die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht (vgl. hierzu die Entschlüsselung „Keine heimliche Online-Durchsuchung privater Computer“, der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007, abgedruckt im 7. TB, Anlage 15). Es muss jedoch nach dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung (vom 27. Februar 2008, Az.: 1 BvR 370/07) durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden, dass sich die Zugriffe auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Da die Strafprozessordnung bislang keine entsprechenden Regelungen enthält, die der Rechtsprechung des Bundesverfassungsgerichts Rechnung tragen, haben die Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschlüsselung der 81. Konferenz am 16./17. März 2011 den Gesetzgeber aufgefordert, Rechtssicherheit zu schaffen (Anlage 15). Nur ein halbes Jahr später wurden Feststellungen des Chaos-Computer-Clubs veröffentlicht, dessen Mitglieder auf einer ihm zugespielten Festplatte mögliche Funktionsweisen einer durchgeführten Quellen-TKÜ-Maßnahme rekonstruiert hatten. Diese legten den Schluss nahe, dass gerade die vom Bundesverfassungsgericht geforderte Beschränkung des Ausspionierens des Computers auf die Telekommunikationsinhalte bewusst oder aus Nachlässigkeit nicht eingehalten wurde. Daran schloss sich eine bundesweite Diskussion über die Frage an, ob und mit welcher Software Quellen-TKÜ bisher durchgeführt worden sind. In diesem Zusammenhang war einer Pressemeldung zu entnehmen, dass in Thüringen kein sogenannter Staatstrojaner eingesetzt wurde. Allerdings hätten Thüringer Behörden in einem Fall das Abhören verschlüsselter Internet-Telefonate beantragt. Trotz Zustimmung des Gerichts sei die Maßnahme dann aber doch nicht durchgeführt worden. Dies hat den TLfD dazu veranlasst, beim TJM um entsprechende Auskünfte zu bitten. Dabei stellte sich heraus, dass die Staatsanwaltschaft Gera beim Amtsgericht Gera einen Beschluss nach § 100 b StPO zur Telekommunikationsüberwachung erwirkt hatte. Das TLKA, das die Maßnahme umsetzen sollte, verfügte jedoch über keine entsprechenden Mittel zur Durchführung und beauftragte deshalb das Bayerische Landes-

kriminalamt, in Amtshilfe den Beschluss des Amtsgerichts Gera zur Quellen-TKÜ umzusetzen. Wer jedoch dafür verantwortlich ist, dass trotz möglicher weitergehender technischer Möglichkeiten auch nur die zulässigen Daten erhoben werden, war zu klären. Die Verfahrensweise war auch Gegenstand von Erörterungen im Innenausschuss des Landtags. Dabei hat der TLfD die Auffassung des TIM geteilt, dass nach den Vorschriften der Amtshilfe die beauftragte Behörde, hier das Bayerische Landeskriminalamt, die Verantwortung für die Rechtmäßigkeit ihrer Ermittlungshandlungen trägt. Fraglich blieb zunächst, ob sich die Staatsanwaltschaft Gera im Rahmen ihrer Sachleitung völlig entsprechender Prüf- und Überwachungspflichten enthalten und die Durchführung vollständig der Polizei überlassen konnte. Hier könnte man erwägen, dass sich die Staatsanwaltschaft Gera im Rahmen ihrer Sachleitung über den Funktionsumfang der Software zumindest im Rahmen des Möglichen hätte informieren und entsprechende ergänzende Weisungen an das Bayerische Landeskriminalamt hätte erteilen müssen. Allerdings ist dabei zu berücksichtigen, dass sich die Staatsanwaltschaften zur Durchführung ihrer Ermittlungsmaßnahmen der Polizeibehörden gerade in technischer Hinsicht bedienen, weil die entsprechenden Kenntnisse in der Regel nicht vorhanden sein können. Hier durfte sich die Staatsanwaltschaft auf den technischen Sachverstand der Polizei verlassen.

Bevor der TLfD diese Einschätzung vornehmen konnte, gab es jedoch Meinungsverschiedenheiten zwischen dem TLfD und dem TJM zu der Frage, ob dem TLfD Einsicht in die Akten des noch laufenden Ermittlungsverfahrens zu gewähren ist. Anlass war die Weigerung des TJM, dem TLfD den Antrag der Staatsanwaltschaft Gera, den Beschluss des Amtsgerichts Gera sowie das Amtshilfeersuchen des TLKA an das Bayerische Landeskriminalamt vorzulegen. Begründet wurde dies damit, dass nach § 477 Abs. 2 Satz 1 StPO eine Auskunftserteilung während der noch laufenden Ermittlungen den Untersuchungszweck gefährden würde. Da es sich um eine bundesrechtliche Norm handele, ginge diese dem Kontrollrecht des TLfD nach § 38 Abs. 1 ThürDSG vor. Diese Ansicht teilte der TLfD nicht. Eine Anwendung der §§ 474 ff. StPO ist bei einer Datenschutzkontrolle durch den TLfD überhaupt nicht gegeben. Diese Vorschriften betreffen lediglich den Fall, dass Auskünfte aus Strafermittlungsakten zu dort näher genannten Zwecken an die jeweils genannten Stellen übermittelt werden dürfen. Regelungen zur Daten-

schutzkontrolle enthalten die §§ 474 ff. StPO nicht, weshalb sie auf die Datenschutzkontrolle durch den TLfD auch nicht anwendbar sind. Einschlägig sind hier die §§ 37 ff. ThürDSG. Dort sind auch abschließend die Ausnahmen der Kontrollbefugnis geregelt. So sind z. B. nach § 38 Abs. 2 Satz 2 ThürDSG dem TLfD keine Auskünfte zu erteilen, wenn das zuständige Landesministerium im Einzelfall feststellt, dass die Auskunft oder Einsicht in Unterlagen oder Akten die Sicherheit des Bundes oder eines Landes gefährden würde. Darauf hat sich das TJM jedoch ausdrücklich nicht bezogen. Nachdem der TLfD diese Verletzung datenschutzrechtlicher Vorschriften formell gemäß § 39 Abs. 1 ThürDSG beanstandet hatte, gab das TJM seinen Widerstand auf und gewährte Einsicht in die Unterlagen.

Die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung muss unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts gesetzlich geregelt und technisch umgesetzt werden können, damit Rechtssicherheit geschaffen wird.

Es muss auch künftig sichergestellt bleiben, dass der TLfD zu Kontrollzwecken Auskunft und Einsicht auch in solche Unterlagen erhält, die sich auf laufende Ermittlungen beziehen.

10.3 Einschränkung der Funkzellenabfrage

Anlässlich von Versammlungen und Gegendemonstrationen am 19. Februar 2011 in Dresden haben die dortigen Strafverfolgungsbehörden unzählige Verkehrsdaten von Mobilfunkverbindungen erhoben. Dadurch sind zehntausende Versammlungsteilnehmer, darunter auch Bundestags- und Landtagsabgeordnete, Rechtsanwälte und Journalisten, aber auch völlig unbeteiligte Anwohner in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Rechtsgrundlage der Funkzellenabfrage ist § 100 g Abs. 2 Satz 2 StPO. Dabei bezieht sich die Maßnahme nicht auf bestimmte Personen. Voraussetzung und ausreichend für die Erhebung von Verkehrsdaten bei den Telekommunikationsanbietern ist das Vorliegen einer Straftat von erheblicher Bedeutung und eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation. Diese Regelung, die 2001 in die StPO eingefügt wurde, ist nach Auffassung der Datenschutzbeauftragten weder hinreichend be-

stimmt noch den heutigen technischen Gegebenheiten entsprechend. Ohne Zutun ihrer Nutzer erzeugen aktuelle Mobilfunkgeräte eine Vielzahl von Verkehrsdaten (Rufnummern von Anrufern und Angerufenen, Uhrzeit), die später bei einer Funkzellenabfrage erhoben werden können. Die unterschiedslose Erfassung aller in einer Funkzelle befindlichen Mobilfunkgerätebesitzer offenbart das Bewegungs- und Kommunikationsverhalten einer Vielzahl von Menschen, die selbst keinerlei Anlass für einen heimlichen massiven staatlichen Eingriff gegeben haben. Die davon Betroffenen können dann auch wegen anderer Rechtsverstöße (z. B. gegen das Versammlungsgesetz) verfolgt werden, für die keinesfalls eine dermaßen eingriffssintensive Maßnahme hätte angeordnet werden können. Vor allem fehlen weitergehende Regelungen zum weiteren Umgang mit den so erlangten Daten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung vom 27. Juli 2011 (Anlage 19) den Bundesgesetzgeber aufgefordert, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken und u. a. dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen sowie die Löschungsvorschriften zu präzisieren. Mit diesem Ziel, § 100 g StPO, hat das Land Sachsen eine Gesetzesinitiative im Bundesrat (BR-Drs. 532/11) eingebracht. Das Ergebnis der Beratungen ist abzuwarten.

Hinzuweisen ist auch auf die Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011 (Anlage 26) als Reaktion auf die Infragestellung der Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaft im Vorfeld einer bzw. nach einer richterlichen Anordnung zur Durchführung einer Funkzellenabfrage. Dies lenkt wieder einmal die Aufmerksamkeit auf die Wichtigkeit einer unabhängigen Datenschutzkontrolle insbesondere auch im Bereich der Strafverfolgung, wenn Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können.

Der Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage muss eingeschränkt werden.

Vorbeugender Grundrechtsschutz ist insbesondere auch bei verdeckten Ermittlungsmaßnahmen Aufgabe der Datenschutzbeauftragten.

10.4 Datenschutzaspekte bei der Überwachung von entlassenen Intensivtätern

Um rückfallgefährdete Sexualstraftäter nach ihrer Haftentlassung überwachen zu können und damit die Allgemeinheit zu schützen, wurde zunächst in Bayern und anschließend auch in den anderen Bundesländern eine sogenannte HEADS-Konzeption eingeführt. HEADS steht für Haftentlassene-Auskunftsdatei-Sexualstraftäter. Die Einordnung eines Probanden und damit die Aufnahme seiner personenbezogenen Daten in die beim TLKA geführte Datei erfolgt im Zusammenwirken der Justiz und Polizeibehörden. Dabei werden personenbezogene Daten der Probanden aus dem Justizvollzug, der Führungsaufsicht/Bewährungshilfe nach der Haftentlassung und auch polizeiliche Erkenntnisse verarbeitet, um weitere Straftaten zu verhindern. Der TLfD wurde am Entwurf der HEADS-Konzeption beteiligt, wobei alle datenschutzrechtlichen Anregungen und Kritikpunkte umgesetzt wurden.

Aufgrund des Urteils des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 17. Dezember 2009 zur nachträglichen Sicherungsverwahrung wurde das Recht der Sicherungsverwahrung neu geregelt (Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung und zu begleitenden Regelungen vom 22. Dezember 2010; BGBl. I S. 2300). Dabei wurden auch führungsaufsichtsrechtliche Befugnisse erweitert. Insbesondere wurde das Instrumentarium der elektronischen Aufenthaltsüberwachung zur Verbesserung der Kontrolle aufenthaltsbezogener Weisungen eingeführt. Hiervon sind Personen betroffen, gegen die nach bisheriger Rechtslage auch von vornherein Sicherungsverwahrung angeordnet werden konnte. Voraussetzungen für die richterliche Anordnung einer elektronischen Aufenthaltsüberwachung sind gemäß § 68 b Abs. 1 Satz 3 StGB, dass eine Verurteilung zu einer Freiheitsstrafe von mindestens drei Jahren oder die Unterbringung in den Maßregelvollzug angeordnet wurde und die Freiheitsstrafe vollständig vollstreckt wurde bzw. die Maßregel sich erledigt hat, die Strafe bzw. die Unterbringung wegen einer schweren Straftat im Sinne des § 66 Abs. 3 Satz 1 StGB (bestimmte Sexualstraftaten gegen Kinder, Jugendliche oder wider-

standsunfähige Personen, gefährliche Körperverletzung) verhängt oder angeordnet wurde, die Gefahr der Begehung einer weiteren derartigen Straftat besteht und die Weisung erforderlich ist, den Verurteilten von der erneuten Begehung einer solchen Straftat abzuhalten.

Nach § 463 a Abs. 4 StPO ist die Erhebung und Speicherung aller Aufenthaltsdaten einschließlich der Daten über Funktionsstörungen des Geräts erlaubt. Lediglich innerhalb der Wohnung der Betroffenen dürfen mit Verweis auf den Kernbereich privater Lebensführung keine über den Umstand der Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden, soweit dies technisch möglich ist. Die weitergehende Verarbeitung der Daten ist an bestimmte, abschließend aufgezählte, eng begrenzte Zwecke gebunden. Die Daten sind gegen unbefugte Kenntnisnahme zu sichern und soweit kein Weisungsverstoß festgestellt wird, nach zwei Monaten zu löschen. Bei Vorliegen der entsprechenden Voraussetzungen ist die elektronische Aufenthaltsüberwachung ortsunabhängig von der jeweils zuständigen Führungsaufsichtsstelle sofort umzusetzen. Die technische Umsetzung der elektronischen Aufenthaltsüberwachung ist an keine bestimmten Vorgaben gebunden, wird aber in der Regel mittels Anlegens einer sogenannten elektronischen Fußfessel oder anderer Geräte durchgeführt. Erfahrungen liegen im Bundesland Hessen vor, die im Rahmen eines Modellprojekts zum Einsatz elektronischer Fußfesseln entstanden sind. Aufgrund dieser Erfahrungen wurde zunächst von drei Ländern ein Staatsvertrag mit dem Land Hessen abgeschlossen, mit dem eine gemeinsame elektronische Überwachungsstelle der Länder (GÜL) in Hessen eingerichtet wurde. Diesem Staatsvertrag ist Ende 2011 auch Thüringen beigetreten. Die GÜL mit Sitz in Bad Vilbel soll Teile der Aufgaben der Führungsaufsicht zur Überwachung der elektronischen Fußfessel übernehmen, wobei die bereits in Hessen existierende Infrastruktur genutzt werden soll. In Bezug auf die Datenverarbeitung sieht der Staatsvertrag vor, dass für die GÜL das hessische Datenschutzgesetz Anwendung findet und die GÜL vom Hessischen Datenschutzbeauftragten kontrolliert wird. Mit der technischen Durchführung der elektronischen Aufenthaltsüberwachung mit GPS bedient sich die GÜL der Hessischen Zentrale für Datenverarbeitung (HZD). Hierbei handelt es sich um eine Datenverarbeitung im Auftrag. Diese erfolgt ebenfalls unter der Kontrolle des Hessischen Datenschutzbeauftragten,

der die Datenschutzbeauftragten der beteiligten Länder zu dem Projekt auf dem Laufenden hält.

Die Verarbeitung personenbezogener Daten im Rahmen der Überwachung entlassener Intensivtäter wird zu gegebener Zeit bei Thüringer Behörden zu überprüfen sein.

11 Gesundheits- und Sozialdatenschutz

11.1 Krankenhausinformationssystem – eine Orientierungshilfe und deren Umsetzung

Seit Ende des Jahres 2009 befasste sich die Unterarbeitsgruppe "Krankenhausinformationssysteme", die aus Mitgliedern der Arbeitskreise "Technik" und "Gesundheit und Soziales" der Datenschutzkonferenz besteht, mit der Erarbeitung einer Orientierungshilfe, die erstmalig bundesweit und trägerübergreifend ein einheitliches Verständnis der datenschutzrechtlichen Anforderungen an den Einsatz von Krankenhausinformationssystemen ermöglicht. Es fanden mehrere Sitzungen statt, in denen auch Experten, Softwarehersteller und Vertreter der Krankenhäuser gehört wurden. Die Datenschutzkonferenz hat auf ihrer 81. Konferenz am 15./16. März 2011 in Würzburg die von der Unterarbeitsgruppe erarbeitete „Orientierungshilfe Krankenhausinformationssysteme“ verabschiedet (Anlage 18). Neben normativen Eckpunkten zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus befasst sich die Orientierungshilfe auch mit technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen.

Diese Orientierungshilfe ist nach dem Willen der Datenschutzbeauftragten als Maßstab bei künftigen Prüfungen und Beratungen zugrunde zu legen. Gleichzeitig erhalten sowohl die Betreiber der Krankenhäuser als auch die Anbieter von Krankenhausinformationssystemen mit der Orientierungshilfe ein Papier, an dem sie die Gestaltung und Konfiguration ihrer Programme ausrichten können. Sie ist abrufbar auf den Seiten des TLfD in der Rubrik der Veröffentlichungen – Orientierungshilfen.

Darauf basierend hat der TLfD alle Krankenhäuser in öffentlicher Trägerschaft zunächst nach ihrer Größe, den Beteiligungsverhältnissen und dem verwendeten Krankenhausinformationssystem befragt. Dabei wurde festgestellt, dass insgesamt sechs verschiedene Krankenhausinformationssysteme zum Einsatz kommen. Jedes dieser Systeme sollte einer datenschutzrechtlichen Prüfung unterzogen werden. Daher wurden datenschutzrechtliche Kontrollen des Krankenhausinformationssystems in den Krankenhäusern in Altenburg, Arnstadt, Greiz, Jena, Nordhausen und Saalfeld durchgeführt. Als erstes Ergebnis lässt sich feststellen, dass die Sensibilität für Daten-

schutz in den Krankenhäusern sehr unterschiedlich ist. Insbesondere im Hinblick auf das Rollen- und Berechtigungskonzept bestehen erhebliche Unterschiede. In vier Krankenhäusern hatten alle Ärzte Zugriff auf alle Daten. Die Pflegekräfte in einem Krankenhaus hatten auch innerhalb ihrer Station uneingeschränkten Zugriff auf alle Arzteinformationen, in allen anderen Krankenhäusern war der Zugriff des Pflegepersonals mehr oder weniger stark eingeschränkt. In zwei Krankenhäusern hatte das Schreibbüro/der Schreibdienst Zugriff auf alle Patientendaten des Krankenhauses. In zwei weiteren Krankenhäusern traf dies, je nach der entsprechenden Organisationseinheit, auf Teile der Schreibkräfte zu.

In einem Krankenhaus bestand die Möglichkeit, sich auf den Stationsrechnern mit einem aus nur drei Stellen bestehenden Passwort einzuloggen, ohne sich allerdings im Krankenhausinformationssystem anmelden zu können. In keinem Krankenhaus existierte ein Merkblatt, mit welchem der Patient darauf hingewiesen wird, dass ihm ein Widerspruchsrecht zur Hinzuziehung von Daten aus früheren abgeschlossenen Behandlungen zusteht. Kein System ermöglichte einen Hinweis für den Fall, dass der Patient der Heranziehung seiner Vorbehandlungsdaten widersprochen hat. In keinem Krankenhaus existierte ein Löschkonzept für elektronische Patientenakten. Es ist davon auszugehen, dass alle Daten seit Einführung der Systeme im Zugriff stehen. Nach Angaben der Krankenhäuser bietet zudem kein System die Möglichkeit, Daten zu sperren. Vier Krankenhausinformationssysteme verfügen über eine Notfallfunktion für Ärzte, die an keine erschwerenden Voraussetzungen geknüpft ist. In einem System existiert wenigstens die Notwendigkeit einer Begründung eines Notfallzugriffs auf die Patientendaten. Es kann aber jede – noch so unsinnige – Antwort gegeben werden. In keinem Krankenhausinformationssystem werden medizinische Daten von Mitarbeitern, die als Patienten im Krankenhaus behandelt werden, vor unberechtigten Zugriffen der Kollegen besonders geschützt. Drei Systeme ermöglichen eine umfassende Protokollierung sowohl ändernder als auch lesender Zugriffe. Allerdings fehlte es in allen Fällen an Vorgaben für eine anlassunabhängige Protokollauswertung. Bei nur vier von sechs Kontrollen konnte das gesetzlich vorgeschriebene Verzeichnis vorgelegt werden.

Der TLfD forderte die Krankenhäuser zur Behebung dieser Mängel auf. Bislang zeigten sich alle Krankenhäuser grundsätzlich bereit, die datenschutzrechtlichen Mängel zu beseitigen. Es wurden Umset-

zungskonzepte mit konkreten Umsetzungsterminen erarbeitet. Nicht alle Mängel können aber vom Krankenhaus selbst beseitigt werden. Einige Änderungen sind nur durch eine Überarbeitung der Systeme durch den Softwarehersteller möglich. Der TLfD unterstützt die Krankenhäuser im Dialog mit den Herstellern. Sobald die Kontrollen abgeschlossen sind, wird es eine Informationsveranstaltung für die Datenschutzbeauftragten aller Krankenhäuser im Zuständigkeitsbereich des TLfD geben. Ziel soll es sein, über die jeweiligen Mängel der Systeme zu informieren und im gemeinsamen Dialog Lösungsmöglichkeiten anzubieten.

Die datenschutzgerechte Gestaltung der Krankenhausinformationssysteme erfordert einen längeren Prozess, den der TLfD weiter begleiten wird.

11.2 Errichtung von Pflegestützpunkten

Grundlage für die Errichtung von Pflegestützpunkten ist der im Rahmen des Pflege-Weiterentwicklungsgesetzes am 1. Juli 2008 in Kraft getretene § 92 c SGB XI. Danach "richten die Pflegekassen und Krankenkassen Pflegestützpunkte ein, sofern die zuständige oberste Landesbehörde dies bestimmt." Das TMSFG bestimmte durch Allgemeinverfügung vom 22. März 2010, dass die Pflegekassen und Krankenkassen in Thüringen zunächst in den vier Planungsregionen entsprechend der Landesregionenverordnung mindestens je einen Pflegestützpunkt einrichten. Zusätzlich ist der bestehende Pilotstützpunkt in Jena zu einem Pflegestützpunkt umzuwandeln. Am 31. August 2011 teilte das TMSFG in Beantwortung der Kleinen Anfrage Nr. 1662 mit, dass in Thüringen durch die Thüringer Kranken- und Pflegekassen unter Beteiligung der Kommunen bisher zwei Pflegestützpunkte – und zwar in Jena und in Nordhausen – errichtet wurden. Träger der Pflegestützpunkte sind die beteiligten Sozialversicherungsträger (Pflegekassen und Krankenkassen) sowie die Träger der Sozialhilfe. Die Pflegestützpunkte haben die Aufgabe, darüber zu informieren, welche Anbieter es für bestimmte Leistungen gibt und pflegerische und sozialer Versorgungs-, Betreuungs- und Beratungsangebote für die Betroffenen zu koordinieren. Von den Pflegestützpunkten werden sensitive Daten der Ratsuchenden (z. B. über gesundheitliche Probleme, Hilfebedarf) verarbeitet. Daher ist es von zentraler Bedeutung, dass die vom Pflegestützpunkt

vorgenommene Verarbeitung personenbezogener Daten für die Betroffenen transparent ist. Der TLfD hat die Pflegestützpunkte aufgefordert, die Betroffenen über die Datenverarbeitung in einem Merkblatt aufzuklären. Dabei wurde auch ein konkreter Vorschlag für die Gestaltung des Merkblattes zur Verfügung gestellt. Die Pflegestützpunkte wurden außerdem darauf hingewiesen, dass der Datenbestand des Pflegestützpunkts sowohl vom örtlichen Sozialhilfeträger wie auch von den Pflegekassen grundsätzlich abzuschotten ist. Darüber hinaus muss sichergestellt werden, dass nicht künftig alle an einer Beratung und Koordination beteiligten Stellen wie Pflegestützpunkt, örtlicher Sozialhilfeträger, Pflegekasse oder Pflegedienst pauschal einen umfassenden Datenbestand über einen Betroffenen speichern. Eine Speicherung der Daten der Ratsuchenden darf beim Pflegestützpunkt nur solange erfolgen, wie dies zur Aufgabenerfüllung des Pflegestützpunkts erforderlich ist. Spätestens drei Jahre nach dem letzten Kontakt mit dem Betroffenen sind die Daten zu löschen. Für den Pflegestützpunkt Jena wurde auf Nachfrage des TLfD mitgeteilt, dass dieser derzeit lediglich als Scharnier zwischen dem Bürger und dem in Betracht kommenden Leistungsträger fungiert. Dort werden keinerlei personenbezogene Daten der Ratsuchenden gespeichert. Der Pflegestützpunkt Nordhausen hat das vorgeschlagene Merkblatt übernommen. Auch die genannten Speicherfristen werden eingehalten. Im Fall der notwendigen Datenerhebung wird in Abstimmung mit den beteiligten Trägern des Pflegestützpunktes eine Einwilligung der betroffenen Person eingeholt.

Der TLfD wird die Einrichtung der Pflegestützpunkte weiter begleiten und kontrollieren, ob die dargelegten datenschutzrechtlichen Vorgaben eingehalten werden.

11.3 Sozialamt muss Daten beim Betroffenen erheben

Immer wieder ist der TLfD mit Fällen befasst, in denen das Sozialamt für die Bearbeitung eines Antrags notwendige Daten, die von dem Antragsteller nicht vorgelegt werden, bei einer dritten Stelle erhebt. Aus Sicht des Sozialamts dient dies der Verfahrensbeschleunigung.

Exemplarisch soll hier ein Fall benannt werden, in welchem dem Sozialamt des Landkreises Saalfeld-Rudolstadt ein Antrag auf Übernahme der freiwilligen Kranken- und Pflegeversicherungsbei-

träge vorlag, ohne dass der Antragsteller dem Antrag die erforderlichen Krankenkassenunterlagen beilegte. Das Sozialamt kontaktierte die betroffene Krankenkasse, um dort Daten über das bestehende Versicherungsverhältnis zu erfragen. Nach dem Sozialgesetzbuch sind Sozialdaten grundsätzlich beim Betroffenen selbst zu erheben. Nur in den gesetzlich normierten Ausnahmefällen darf sich das Sozialamt zum Einholen von Informationen an Dritte wenden. Diese Voraussetzungen lagen in dem konkreten Fall nicht vor. Wer Sozialleistungen beantragt, hat nach § 60 Abs. 1 Satz 1 Nr. 1 SGB I alle Tatsachen anzugeben, die für die Leistung erheblich sind und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte, bspw. einer Krankenkasse, zuzustimmen. Sofern der Antragsteller der Datenerhebung bei der dritten Stelle nicht zustimmt, ist das Sozialamt nicht zur Erhebung befugt, sondern muss den Leistungsantrag ablehnen. Darauf wurde das Sozialamt hingewiesen und aufgefordert, zukünftig entsprechend zu verfahren.

Auch wenn die Erhebung von Daten durch das Sozialamt bei Dritten der Bescheidung eines gestellten Leistungsantrags dient, ist grundsätzlich immer vorab die Zustimmung des Betroffenen hierzu einzuholen.

11.4 Rote Windelsäcke für Inkontinente

Nach der Abfallgebührensatzung des Landkreises Schmalkalden-Meinungen können pflegebedürftige Personen ebenso wie Haushalte mit Kleinstkindern pro Jahr eine bestimmte Anzahl verbilligte, farblich besonders gekennzeichnete Windelsäcke erhalten. Daneben können für sonstigen zusätzlichen Abfall Müllsäcke in einer anderen, neutralen Farbe erworben werden. Diese Müllsäcke können zusätzlich zur normalen Mülltonne verwendet werden und sind neben der Mülltonne zur Abholung bereitzustellen. Die Pflegebedürftigkeit sollte im Einzelfall durch die Vorlage von Kopien des Lieferscheins des Sanitätshauses, des Rezepts oder einer ärztlichen Bescheinigung nachgewiesen werden. Dieses sicher gutgemeinte Angebot stellt in datenschutzrechtlicher Hinsicht ein Problem dar. Zum einen ist die Forderung der Vorlage eines Rezepts nicht angemessen, weil sich auf ihm auch andere ärztliche Verordnungen befinden können, die Rückschlüsse auf den Gesundheitszustand des Pflegebedürftigen

zulassen. Zum anderen deutet die Farbe des an der Straße zur Abholung bereitgestellten verbilligten Windelsacks darauf hin, dass sich dort eine pflegebedürftige, wahrscheinlich inkontinente Person aufhält, insbesondere bei Haushalten, in denen sich keine Kleinstkinder aufhalten. Der TLfD wies gegenüber dem zuständigen Landratsamt auf diesem Umstand hin. Das Landratsamt legte dar, dass die Abfallsatzung des Landkreises nicht kurzfristig geändert werden könne. Es wurde für eine Übergangszeit vereinbart, dass pflegebedürftige Personen bei der Antragstellung mitteilen könnten, dass sie keine farblich gekennzeichneten, sondern die neutralen Säcke wünschten. Der TLfD wirkte darauf hin, dass in das entsprechende Antragsformular ein solcher Hinweis aufgenommen wird. Der TLfD hat gegenüber dem Landkreis darauf gedrungen, dass die Abfallsatzung noch im Jahr 2011 geändert wird. Daraufhin änderte der Landkreis seine Abfallsatzung. Pflegebedürftige Personen erhalten nunmehr vergünstigte Abfallsäcke in der neutralen Farbe, die auch die übrigen Müllsäcke haben. Mit dem entsprechenden schriftlichen Antrag sind „geeignete Nachweise“ zu führen. Dies können bspw. auch Rechnungen eines Sanitätshauses sein.

Eine Datenschutzverletzung kann auch darin bestehen, dass durch eine farbliche Kennzeichnung von Müllsäcken Rückschlüsse auf den Gesundheitszustand der sie Benutzenden gezogen werden können.

11.5 Vertretung des Amtsarztes durch Private

Eine an den TLfD herantragene Bürgeranfrage ergab, dass zumindest im Landkreis Altenburger Land die schulzahnärztlichen Reihenuntersuchungen nicht nur von den Schulzahnärzten des Gesundheitsamts, sondern auch von privaten Zahnärzten durchgeführt werden. Das betreffende Gesundheitsamt teilte mit, dass die regulär beschäftigten Zahnärzte mehrwöchig arbeitsunfähig gewesen seien. Da die zahnärztliche Aufgabenerfüllung mit den angestellten Zahnärzten des Fachdienstes Gesundheit nicht mehr möglich gewesen sei, habe der Landkreis zwei privat tätige Zahnärzte mit Honorarverträgen beschäftigt.

Dies begegnet nach Ansicht des TLfD erheblichen datenschutzrechtlichen Bedenken. Nach § 55 Abs. 3 ThürSchulG sind die Schüler verpflichtet, sich den Maßnahmen des schulärztlichen und schulzahnärztlichen Dienstes zu unterziehen. Bei einer Untersuchung

durch den „Schulzahnarzt“ werden die Schüler nicht nur körperlich untersucht, es werden auch (Gesundheits-)Daten 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 TLfD hat dem TMSFG als oberste Aufsichtsbehörde seine Rechtsauffassung dargelegt und angeregt, die Gesundheitsämter in einem entsprechenden Rundschreiben über die Rechtslage aufzuklären. Die Reaktion des TMSFG steht noch aus.

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 nur von Trägern hoheitlicher Gewalt durchgeführt werden.

11.6 Datensparsame Umsetzung des Bildungspaketes?

Zum 1. Oktober 2011 ist das sogenannte Bildungspaket in Kraft getreten. Es war in dem Gesetz zur Ermittlung von Regelbedarfen und zur Änderung des SGB II und XII enthalten. Nach den neuen Regelungen im SGB II und XII erhalten hilfebedürftige Kinder, Jugendliche und junge Erwachsene u. a. Leistungen für die Teilnahme an Ausflügen, für den Schulbedarf, die Schülerbeförderung, Nachhilfe, Mittagsverpflegung und die Mitgliedschaft in Vereinen. Das Gesetz sieht vor, dass die Leistungen für Bildung und Teilhabe insbesondere in Form von personalisierten Gutscheinen oder Direktzahlungen an Anbieter von Leistungen erbracht werden. Die Träger bestimmen dabei selbst, in welcher Form sie die Leistungen erbringen. Leistungen aufgrund des Bildungspaketes können ALG II-

Empfänger und Sozialhilfe-Empfänger erhalten. Örtliche Träger der Sozialhilfe sind nach § 3 Abs. 2 SGB XII die kreisfreien Städte und Kreise. Träger der Leistungen nach dem SGB II ist grundsätzlich die Agentur für Arbeit, sofern nicht ein Landkreis oder eine Kreisfreie Stadt von der Möglichkeit der Zulassung kommunaler Träger nach § 6 a SGB II Gebrauch gemacht hat. In Thüringen trifft dies auf die Stadt Jena und den Landkreis Eichsfeld zu (s. u. 11.7). Da das Verfahren zur Inanspruchnahme des Bildungspakets datenschutzgerecht zu gestalten ist, hat der TLfD alle Sozialämter und die zwei seiner Kontrolle unterliegenden Jobcenter um Mitteilung darüber gebeten, wie sie das Bildungspaket umsetzen. Nach der Auswertung der Rückläufe wurde es als datenschutzrechtlich problematisch angesehen, dass in zwei Fällen Gutscheine ausgeteilt wurden, in die sich mehrere Leistungserbringer eintragen sollten. Hierdurch bekommt ein Leistungserbringer, der sich zu einem späteren Zeitpunkt einträgt, unzulässigerweise Informationen über das Konsumverhalten des Berechtigten. In beiden Fällen wurden die Gutscheine auf Intervention des TLfD geändert. In einer Behörde mussten Antrag und die Bestätigung durch die Einrichtung in einem Formular vorgenommen werden. Hier wurde um Änderung gebeten, weil ansonsten der Leistungserbringer, ohne dass hierfür eine Notwendigkeit besteht, Kenntnis über die Anspruchsgrundlage für die Leistung erhält und damit bspw. erfährt, ob jemand Sozialhilfe oder ALG II erhält. Gleiches gilt, wenn der Leistungsberechtigte dem Leistungserbringer den Bewilligungsbescheid zum Nachweis seiner Berechtigung vorlegen muss. Sofern dies der Fall war, veranlasste der TLfD, dass die Leistungsberechtigten auf Verlangen eine neutrale Kostenübernahmeerklärung erhalten. In vielen Fällen waren die datenschutzrechtlichen Hinweise für die Leistungserbringer nicht vorhanden bzw. nicht hinreichend. Hier hat der TLfD Hinweise zur datenschutzgerechten Gestaltung gegeben. Die Ergebnisse waren ansonsten aber aus datenschutzrechtlicher Sicht positiv. Die Abrechnung erfolgte in der Mehrzahl der Fälle nicht über Gutscheine, sondern mit dem Leistungserbringer direkt, wobei nur die jeweils notwendigen Daten übermittelt wurden.

Wenn im Rahmen der Gewährung von staatlichen Leistungen Dritte als Leistungserbringer eingebunden werden, sind nur die personenbezogenen Daten an sie zu übermitteln, die zur Wahrnehmung ihrer Aufgabe erforderlich sind.

11.7 Zuständigkeitswechsel bei den Jobcentern

Im Bereich der Gewährung von Arbeitslosengeld (ALG) II haben sich mit dem Ablauf des Jahres 2010 durch das Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende vom 3. August 2010 (BGBl. I 2010, S.1112) die Zuständigkeiten geändert. Zunächst ist zu erwähnen, dass die Arbeitsgemeinschaften (ARGE) nun Jobcenter heißen, (§ 6 d SGB II). Diese Jobcenter betreuen die Bezieher von ALG II sowohl im Hinblick auf die Leistungsgewährung als auch hinsichtlich der Vermittlung von Arbeit. Nach dem gesetzlichen Regelfall sind die Jobcenter als gemeinsame Einrichtungen zwischen der Agentur für Arbeit und Kommune (Landkreise und kreisfreie Städte) eingerichtet. Demgegenüber wird einigen Kommunen die Option eingeräumt, alle Aufgaben nach dem SGB II eigenständig wahrzunehmen (sogenannte zugelassene kommunale Träger – Optionskommunen – gemäß § 6 a bis § 6 c SGB II). Seit dem 1. Januar 2011 ist die datenschutzrechtliche Zuständigkeit für alle Jobcenter grundsätzlich auf den BfDI übergegangen, (§ 50 Abs. 4 Satz 3 SGB II). Demgegenüber unterliegen die Jobcenter der zugelassenen Optionskommunen weiterhin der Kontrolle der Landesbeauftragten für den Datenschutz. In Thüringen betrifft dies die kreisfreie Stadt Jena und den Landkreis Eichsfeld. Ab dem 1. Januar 2012 werden der Landkreis Greiz und der Landkreis Schmalkalden-Meiningen hinzukommen.

Aufgrund des Zuständigkeitswechsels hat sich der Arbeitsaufwand des TLfD im Bereich der Jobcenter/ARGEN quantitativ verringert. Gleichwohl ist die datenschutzrechtliche Kontrolle der in seiner Zuständigkeit verbleibenden Optionskommunen weiterhin ein wichtiges Thema. Auf diesem Gebiet ist jedoch aus Gründen Einheitlichkeit der Rechtsanwendung eine verstärkte Abstimmung mit dem BfDI erforderlich.

11.8 Datenhungrige ARGE

Die ARGE Erfurt nahm es noch im Jahr 2010 mit dem Sammeln von Daten zu genau. Eltern beschwerten sich, dass Zeugniskopien von ihrem 14-jährigen Kind im Rahmen der Antragstellung für das ALG II vorgelegt werden sollten. Die ARGE begründete dies auf

Nachfrage des TLfD damit, dass nach § 3 Abs. 2 Satz 1 SGB II erwerbsfähige Hilfsbedürftige, die das 25. Lebensjahr noch nicht vollendet haben, unverzüglich nach Antragstellung in eine Arbeit, eine Ausbildung oder eine Arbeitsgelegenheit zu vermitteln sind. Es könne davon ausgegangen werden, dass das Kind mit Abschluss des Schuljahres 15 Jahre alt wird und in eine Ausbildung vermittelt werden kann. Diese Auffassung teilte der TLfD nicht. Gemäß einem Schreiben der Bundesagentur für Arbeit an den BfDI können durch das Jobcenter „im Einzelfall“ Schulbescheinigung, Kopien von Schulzeugnissen sowie ein ausgefülltes umfassendes Arbeitspaket von einem Minderjährigen angefordert werden. Dies bedeutet, dass nicht regelmäßig und ohne begründeten Anlass die Schulzeugnisse von Schülern abgefordert werden dürfen, die nachweislich an einer Schule angemeldet sind und diese auch weiterhin besuchen wollen. Die Vorlage einer Schulbescheinigung ist zu dem verfolgten Zweck ausreichend. Daraufhin kündigte die ARGE an, ab sofort darauf zu verzichten, von jugendlichen Neukunden bereits per Anschreiben zum Anmeldebogen für die Antragstellung generell eine Zeugniskopie abzufordern. Allerdings hält sich die ARGE nach wie vor dazu berechtigt, eine Vermittlung in Ausbildung anzubieten. Damit die ARGE dies leisten könne, müsse das persönliche Profil des Jugendlichen Berücksichtigung finden und hierzu gehörten auch die schulischen Kenntnisse. Die Vorlage des aktuellen Schulzeugnisses sei ab dem Eintritt des jugendlichen Ausbildungssuchenden in das Schulentlassungsjahr erforderlich, um dem gesetzlichen Auftrag nach Ausbildungsvermittlung in der gebotenen Qualität nachzukommen. Der ARGE wurde nochmals mitgeteilt, dass der TLfD nach wie vor keine Veranlassung dafür sieht, bei Jugendlichen, die eine weiterführende Schule besuchen wollen, in die Zeugnisse Einsicht zu nehmen. Dies wäre nur dann zulässig, wenn keine Schulbesuchsbescheinigung mehr vorgelegt werden würde oder andere Hinweise dafür sprächen, dass kein regelmäßiger Schulbesuch erfolge. Diese Frage konnte mit der ab 2011 unter Jobcenter Erfurt firmierenden Stelle nicht mehr zu Ende diskutiert werden, da sie seither in die Zuständigkeit des BfDI fällt (s. o. 11.7).

ARGEN bzw. Jobcenter dürfen nur die Daten erheben, die für Ihre Aufgabenwahrnehmung wirklich erforderlich sind. Solange ein Jugendlicher nachweislich eine Schule besucht, ist die Vorlage eines Schulzeugnisses für das ALG II nicht notwendig.

11.9 Mindestanforderungen bei Anbindung an medizinische Netze

Im medizinischen Bereich gibt es schon immer besonders hohe Datenschutzerfordernungen, die sich bereits aus der Schweigepflicht (§ 203 StGB) des Arztes ergeben. Diese Anforderungen resultieren aus der hohen Sensibilität der anfallenden medizinischen und persönlichen Daten von Patienten und werden auch nur in den seltensten Fällen in Frage gestellt. Zu Abrechnungs-, Behandlungs- und Dokumentationszwecken muss ein Teil dieser Daten mithilfe von Netzwerken an andere Stellen, wie bspw. die Kassenärztliche Vereinigung, übermittelt werden (§ 295 Abs. 4 SGB V i. V. m. den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung). Um den hohen Anforderungen an Sicherheit und Datenschutz in den Kommunikationsnetzen gerecht werden zu können, muss entsprechend dem Stand der Technik der gesamte Datenverkehr im Netz verschlüsselt werden. Wesentliche Anforderungen an medizinische Daten wie Integrität, Verfügbarkeit, Vertraulichkeit, Authentizität, Nichtabstreitbarkeit und die Originalität können mit der Authentifizierung von Sender und Empfänger und der Verschlüsselung von Kommunikationswegen erreicht werden. Ebenfalls muss ein unbefugter Zugriff auf das lokale Netz in den medizinischen Einrichtungen ausgeschlossen sein. Hierzu sind entsprechende technische und organisatorische Maßnahmen – wie bspw. Zugangs- und Zugriffsregelungen – zu schaffen die eine unbefugte Nutzung der Patientendaten verhindern.

Auf der 81. Konferenz der Datenschutzbeauftragte des Bundes und der Länder wurden die Mindestanforderungen in einer Entschließung „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ verabschiedet (Anlage 14).

Aufgrund des hohen Schutzbedarfes sensibler Patientendaten muss im Rahmen der Rechtsvorschriften und der zunehmenden Vernetzung von lokalen medizinischen Netzen der unbefugte Zugriff durch geeignete Maßnahmen verhindert werden.

12 Wirtschaft, Arbeit, Bau und Verkehr

12.1 Solarkataster zur Solarpotentialanalyse

Verschiedene Städte und Landkreise in Thüringen planen die Erstellung eines Solarkatasters, welches im Internet ohne weitere Zugangsvoraussetzungen veröffentlicht werden soll. Zu diesem Zweck werden Luftbildaufnahmen vom jeweiligen Gemeindegebiet so bearbeitet, dass alle Dachflächen von Gebäuden je nach Eignungsgrad für die Nutzung von Solarenergie unterschiedlich farblich gekennzeichnet werden. Aus datenschutzrechtlicher Sicht werden mit dem Kataster Angaben zu Ort, Straße, Hausnummer und die Einschätzung der Solareignung bekannt gegeben, die personenbezogen, in jedem Fall aber durch Rückschlüsse auf den Grundstückseigentümer personenbeziehbar sind. Gemäß § 4 Abs. 1 ThürDSG 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 das Solarkataster eine Umweltinformation i. S. v. § 2 Abs. 3 Nr. 3 b Thüringer Umweltinformationsgesetz (ThürUIG) darstellt, ist zu prüfen, ob hiernach die Voraussetzungen für eine Veröffentlichung eines Solarkatasters vorliegen. Gemäß § 10 Abs. 6 ThürUIG i. V. m. § 9 Abs. 1 ThürUIG ist eine Unterrichtung der Öffentlichkeit bei einer Beeinträchtigung des Schutzes privater Belange abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse überwiegt. Die Förderung erneuerbarer Energien stellt ohne Zweifel ein öffentliches Interesse dar. Bei der Abwägung zwischen dem schutzwürdigen Interesse des Betroffenen und dem öffentlichen Interesse ist aber zu fragen, worin denn das öffentliche Interesse liegen soll, dass jedermann sich nicht nur über die Solareignung seines eigenen Daches, sondern beliebig vieler Dächer informieren kann. Der Hauseigentümer hat vielmehr z. B. ein überwiegendes schutzwürdiges Interesse daran, nicht von personenbezogenen Werbemaßnahmen der Solarbranche überschüttet zu werden. Der TLfD sieht daher in der Internetveröffentlichung der Solarkataster ohne vorherige Einwilligung der Betroffenen einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht. Die Gemeinde ist hingegen nicht gehindert, den Hauseigentümern für die eigenen Gebäudedächer eine Solarpotentialanalyse zur Verfügung zu stellen.

Solarkataster dürfen nur dann im Internet veröffentlicht werden, wenn zuvor die Einwilligung des Gebäudeeigentümers eingeholt wurde. Keine Bedenken bestehen gegen die Einsichtnahme in die Solarpotentialanalyse der jeweils eigenen Dachfläche.

12.2 Intelligente Stromzähler – neueste Entwicklungen

Wie der TLfD über die Einführung von Intelligenten Stromzählern, den sogenannten „Smart Metern“, berichtete (8. TB, 12.4), waren die Messstellenbetreiber seit dem 1. Januar 2010 verpflichtet, in Privathaushalten gemäß § 21 b Abs. 3 a Energiewirtschaftsgesetz (EnWG) solche Messeinrichtungen anzubieten. Inzwischen ist das EnWG aber durch das Gesetz zur Neuregelung energiewirtschaftlicher Vorschriften vom 28. Juli 2011 geändert worden. Nach wie vor hält der Bundesgesetzgeber daran fest, moderne, intelligente Messsysteme zur Erfassung elektrischer Energie in den privaten Haushalten einzuführen. Die Verpflichtung, dies ab dem 1. Januar 2010 nach und nach umzusetzen, wurde allerdings fallen gelassen. Mit der Gesetzesänderung „erfolgte eine grundsätzliche Neuausrichtung im Sinne erster Grundlagen für ein Smart Metering, das Anforderungen von Datenschutz und Datensicherheit genügt.“ (BT-Drs. 17/6072, S. 76) Geblieben ist zwar weiterhin die Verpflichtung, die genannten Messsysteme einzubauen. Die Einbauverpflichtung beginnt aber frühestens, wenn zertifizierte Geräte am Markt verfügbar sind, womit nicht vor Herbst 2012 zu rechnen ist. Darüber hinaus ist nach § 21 i EnWG mit der Erstellung weiterer Rechtsvorschriften zu rechnen, in denen die nähere Ausgestaltung der Messsysteme hinsichtlich ihrer Mindestfunktionalitäten geregelt werden wird. Selbst wenn der Einbau von Smart Metern erfolgt ist, so ist dies nicht gleichbedeutend mit der Nutzung der Fernauslesung von Verbrauchsdaten. Nach § 21 g Abs. 6 Satz 5 EnWG dürfen Fernwirken und Fernmessen „nur vorgenommen werden, wenn der Letztverbraucher zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach Unterrichtung eingewilligt hat.“ Aus datenschutzrechtlicher Sicht ist diese Regelung sehr zu begrüßen. Damit werden wesentliche Forderungen der Entschließung auf der 80. Konferenz der Datenschutzbeauftragten am 3./4. November 2011 „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs (Anlage 11) umge-

setzt. Es bleibt die Widersprüchlichkeit der Regelung, dass einerseits die intelligenten Messsysteme einzubauen sind, andererseits der Kunde keinen Gebrauch von deren Funktionalitäten machen muss.

Mit dem geänderten EnWG hat der Gesetzgeber auf die datenschutzrechtlichen Probleme reagiert, die sich aus der Einführung von Smart Meter ergeben. Es sind aber noch die erforderlichen Rechtsverordnungen und technischen Richtlinien zu erlassen. Der TLfD behält die Entwicklungen im Auge, einschließlich einer etwaigen „Opt-Out-Lösung“.

12.3 Stadtwerke Erfurt verlangten unnötige Daten als Nachweis

Im Rahmen einer Beschwerde wurde mitgeteilt, dass die Stadtwerke Erfurt GmbH bei einem Kundenwechsel infolge eines Grundstücksverkaufs den bisherigen Kunden um die Offenlegung des betreffenden Kaufvertrags gebeten hatte. Dies wurde unter Hinweis auf § 32 Abs. 4 der Allgemeinen Bedingungen für die Versorgung mit Wasser (AVBWasserV) damit begründet, dass nur auf diesem Wege eine Umschreibung des Versorgungsvertrages vorgenommen werden könne. Nach § 32 Abs. 4 AVBWasserV ist ein Wechsel in der Person des Kunden dem Wasserversorgungsunternehmen unverzüglich mitzuteilen und bedarf der Zustimmung des neuen Kunden. Das Unternehmen ist nicht verpflichtet, dem Eintritt des Dritten in die sich aus dem Vertragsverhältnis ergebenden Rechte und Pflichten zuzustimmen. Eine Verpflichtung eines Neukunden, den betreffenden Kaufvertrag gegenüber dem Versorgungsunternehmen zu offenbaren, ist der o. g. Rechtsnorm jedoch nicht zu entnehmen. Gemäß § 19 Abs. 1 ThürDSG dürfen personenbezogene Daten nur erhoben werden, wenn sie zur Aufgabenerfüllung der erhebenden Stelle erforderlich sind. Nach § 19 Abs. 1 ThürDSG i. V. m. § 32 Abs. 4 AVBWasserV dürfen daher nur personenbezogene Daten erhoben werden, die dem Nachweis des Wechsel des Grundstückseigentümers bzw. Kunden gegenüber dem Wasserversorger dienen. Die im Musterschreiben der Stadtwerke Erfurt GmbH verwendete Formulierung „... Um den Kundenwechsel bearbeiten zu könne, bitten wir uns eine Kopie des Kaufvertrages zur Verfügung zu stellen ...“ sowie die darin genannten Rechtsgrundlagen entsprachen nicht den datenschutzrechtlichen Anforderungen. Der Stadtwerke Erfurt

GmbH wurde mitgeteilt, dass ein Nachweis des Eigentumsübergangs mittels eines aktuellen Grundbuchauszugs bzw. einer auszugsweisen Kopie des Kaufvertrages nur dann keinen Bedenken begegnet, wenn unter Berücksichtigung der datenschutzrechtlich gebotenen Transparenz folgende Voraussetzungen eingehalten werden:

- Der Regelungsgehalt des § 32 Abs. 4 AVBWasserV sollte – nach Möglichkeit unter vollständiger Nennung der Verordnungsbezeichnung – genannt werden.
- Auf die Möglichkeit, auch einen aktuellen Grundbuchauszug vorzulegen, sollte hingewiesen werden.
- Die spezielle Intention der Vorlage des Kaufvertrags sollte verdeutlicht werden.
- Auf die Möglichkeit, eine Schwärzung der nicht den Eigentümerwechsel betreffenden Daten vorzunehmen, sollte hingewiesen werden.

Nachfolgend wurde entsprechend der Hinweise das verwendete Musteranschreiben überarbeitet.

Die Beschränkung des Datenumfangs auf den zur Aufgabenerfüllung erforderlichen Umfang sowie die aus dem Transparenzgebot abgeleitete Klarheit und Verständlichkeit sind wichtige Leitlinien zur Formulargestaltung.

12.4 Weitergabe von Daten aus dem Gewerberegister

Das Gewerbeamt der Stadt Pößneck beabsichtigte, dem Landratsamt zum dortigen Aufbau einer Unternehmensdatei sowie einer für die Wirtschaftsförderung zuständigen, ausgegliederten Stelle in Form einer GmbH regelmäßig Gewerbedaten (Name, Anschrift und Tätigkeit) zu übermitteln und diese auch im Internet zu veröffentlichen. Der TLfD teilte dem Gewerbeamt hierzu mit, dass mit der Änderung der Gewerbeordnung vom 22. August 2006 (Erstes Mittelstandsentlastungsgesetz) und der Neufassung des § 14 GewO die Auskunftserteilung aus dem Gewerberegister zwar erleichtert worden ist, die drei Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) nach § 14 Abs. 5 Satz 2 GewO allgemein zugänglich sind und die Gewerbebehörden im Regelfall die Auskunft dieser Daten nicht versagen dürfen. Die Zulässigkeit einer Veröffent-

lichung aller Gewerbetreibenden mit Name, betrieblicher Anschrift und angezeigter Tätigkeit im Internet ergibt sich hieraus aber nicht. Dies ist den Regelungen des § 14 GewO zwar nicht unmittelbar, aber unter Heranziehung der amtlichen Begründung zu § 14 Abs. 11 GewO zu entnehmen. In der BR-Drs. 68/07 heißt es auf S. 95: „Um dem Regelungszweck, zu verhindern, dass die nicht-öffentlichen Stellen in den Grunddaten aus den Gewerbeanzeigen wie in einem elektronischen Branchenverzeichnis nach beliebigen Suchkriterien recherchieren können, Rechnung zu tragen, werden die einzelnen Voraussetzungen, wie etwa die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung des gesuchten Gewerbetreibenden und der zulässige Umfang der an die ersuchende Stelle zu übermittelnden Treffer in den allgemeinen Verwaltungsvorschriften der Länder zu regeln sein.“ Wäre eine Internetveröffentlichung erlaubt, wären die Regelungen zur Datenübermittlung im automatisierten Abrufverfahren (Absätze 11 und 12) nicht erforderlich. Die Grunddaten dürfen also ohne weitere Voraussetzungen nur im Einzelfall, ggf. auch fallweise übermittelt bzw. zum Abruf bereitgestellt werden. Weiterhin werden in § 14 Abs. 8 GewO diejenigen öffentlichen Stellen benannt, denen die zuständige Behörde regelmäßig Daten aus den Gewerbeanzeigen übermitteln darf. Zudem dürfen nach § 14 Abs. 5 Satz 1 GewO die erhobenen Daten nur für die Überwachung der Gewerbeausübung sowie statistische Erhebungen verwendet werden. Da keine Rechtsvorschrift die Verarbeitung von Gewerbedaten zu Zwecken der Wirtschaftsförderung vorsieht, ist die regelmäßige Übermittlung dieser Daten nicht erlaubt.

Die allgemeine Zugänglichkeit zu den drei Grunddaten des Gewerberegisters bedeutet nicht, dass diese Daten im Internet veröffentlicht werden oder einer anderen beliebigen öffentlichen Stelle regelmäßig übermittelt werden dürfen.

12.5 Neues Einlasssystem an der Ski-Arena Silbersattel

Aufgrund einer Bürgereingabe wurde der TLfD auf ein Kontrollverfahren am Sesselskilift an der Ski-Arena Silbersattel der Stadt Steinach aufmerksam. Das neue Einlasssystem besteht aus einem Drehkreuz, welches einen Höhensensor zur Bestimmung des Überschreitens einer bestimmten Körpergröße enthält. Es ist mit einer

Kamera ausgestattet, die im Moment der Freigabe des Drehkreuzes beim Erkennen einer gültigen Saison-, Mehrtages- oder Tagesliftkarte durch ein kontaktloses Auslesen mittels eines RFID-Chips ein Foto des Skifahrers erstellt. Stundenliftkarten lösen keine Aufnahme aus. Die Bilder werden auf einem in der Lifthütte befindlichen Computer gespeichert. Der Liftwart hat die Möglichkeit, die zu einer bestimmten Liftkarte erstellten Fotos miteinander zu vergleichen. So würden z. B. Erwachsene den verbilligten Kindertarif nutzen oder die personengebundene Liftkarte würde an andere Skifahrer weitergereicht bzw. –verkauft. Als Alternative zur Fotoüberwachung wäre eine dauerhafte und flächendeckende Kontrolle der Skipässe durch das Liftpersonal erforderlich gewesen, was aber durch den großen Andrang an Skifahrern zu langen Wartezeiten am Lift geführt hätte. Der Nachweis, dass mehrere Skifahrer sich eine Liftkarte „teilen“, sei bis zur Einführung des Fotoabgleichs praktisch nicht möglich gewesen. Entsteht bei dem Abgleich mehrerer Aufnahmen der Verdacht auf eine Beförderungserschleichung, wird der Betroffene vom Liftpersonal zur Rede gestellt. Auf Nachfrage bei der Stadt Steinach habe sich die Skiarena Silbersattel Steinach GmbH für dieses Verfahren entschieden, weil in den vorangegangenen Saisons festgestellt werden musste, dass zahlreiche „Schwarzfahrer“ den Sessellift nutzten und dem Betreiber der Skiarena hierdurch in einer Saison Einnahmen im fünfstelligen Bereich entgehen.

Mit diesem neu eingeführten Kontrollsystem liegt eine Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen vor. Da die Stadt Steinach als Eignerin der Silbersattel GmbH insoweit am Wettbewerb mit anderen Skigebieten teilnimmt, kommt gemäß § 26 ThürDSG das BDSG zur Anwendung. Die Zulässigkeit der Bildüberwachung ergibt sich aus § 6 b Abs. 1 Nr. 3 BDSG. Danach ist die Beobachtung öffentlich zugänglicher Räume mit einer solchen Einrichtung zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die erstellten Aufnahmen werden täglich, mit Ausnahme der Saisonkarten, mit einem automatisierten Verfahren gelöscht, indem das Zugangssystem jeden Tag neu gestartet wird. Zugang zu den Bilddaten in der Lifthütte haben nur das Lift- und Kassenpersonal, am Drehkreuz ist ein Hinweis Piktogramm angebracht, im Kassenbereich sind die AGBs angebracht. Das Verfahren und der Umgang mit den gespeicherten Fotos sind in einer

Dienstanweisung geregelt. Auf Forderung des TLfD wurden die AGBs höher angebracht, damit die Erkennbarkeit für die Liftbenutzer gewährleistet ist.

Eine Bildüberwachung ist zur Wahrnehmung eines wirtschaftlichen Interesses einer Stelle zulässig, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Nach Würdigung der Gesamtumstände bestehen seitens des TLfD gegen das beschriebene Verfahren keine Einwände.

12.6 Kfz-Halterauskunft über Umwege nicht zulässig

Ein Mieter wunderte sich darüber, dass seine Wohnungsgesellschaft Kenntnis über die Halterdaten des von ihm gefahren PKWs hatte, welcher auf einem zur Wohnung gehörenden privaten Parkplatz abgestellt war und wandte sich an den TLfD mit der Frage, in welchen Fällen die Kfz-Halterdaten von der Zulassungsstelle an Dritte übermittelt werden dürfen. Eine entsprechende Anfrage bei der zuständigen Stelle ergab, dass die Halterdaten nicht direkt an den o. g. Wohnungsvermieter, sondern an das Ordnungsamt der Stadt Sondershausen übermittelt wurden. Die Zulassungsstelle hatte zu diesem Zeitpunkt keine Kenntnis über den Grund der Datenanfrage und ging von einer Zulässigkeit dieser Übermittlung gemäß § 33 Abs. 1 StVG aus, wonach die dort gespeicherten Daten an Behörden und sonstige öffentliche Stellen zur Verfolgung von Ordnungswidrigkeiten übermittelt werden dürfen. Da stets die Daten anfordernde Stelle die Verantwortung für die Zulässigkeit der Anfrage hat, war gegenüber der Zulassungsstelle somit kein datenschutzrechtlicher Verstoß festzustellen. Allerdings hatte das Ordnungsamt die Halterdaten an einen privaten Dritten zur Geltendmachung eines möglichen privaten Rechtsanspruchs ohne ersichtliche Rechtsgrundlage übermittelt. Der TLfD stellte gegenüber dem Ordnungsamt klar, dass zwar die Zulassungsstelle nach § 39 Abs. 3 StVG Halterdaten an einen Empfänger unter den dort genannten Voraussetzungen übermitteln durfte, dem Ordnungsamt dies aber nicht erlaubt war, da dies ein Verstoß gegen die ursprüngliche Übermittlungsvoraussetzung darstellte.

Wenn öffentlichen Stellen Daten zu einem gesetzlich festgelegten Zweck übermittelt werden, so dürfen diese die Daten grundsätzlich nicht an private Dritte weiter übermitteln werden.

12.7 Verkehrszählung per Video in Bad Lobenstein

Aufgrund eines Zeitungsartikels sowie einer darauf bezogenen Presseanfrage hatte sich der TLfD mit einer speziellen Anwendung von Videoüberwachung zu befassen. Das Straßenbauamt Ostthüringen installierte zu Zwecken einer Verkehrszählung an einem Verkehrsknotenpunkt eine aus mehreren Kameras bestehende Videoanlage. Ziel der Maßnahme war die Beobachtung des Verkehrsflusses, um daraus Erkenntnisse für erforderliche bauliche Veränderungen zu gewinnen. Dabei wurde das Verkehrsgeschehen mit einem digitalen Videorecorder aufgezeichnet, um die Aufnahmen zu einem späteren Zeitpunkt in der Behörde auszuwerten.

Da es sich bei der Videoüberwachung um einen wesentlichen Eingriff in das Persönlichkeitsrecht der Betroffenen handelt, kann die Zulässigkeit für die Durchführung dieser Maßnahme nicht mit den im ThürDSG allgemein geregelten Zulässigkeitsvoraussetzungen über die Erhebung und Verarbeitung personenbezogener Daten – bspw. mit § 19 Abs. 1 bzw. § 20 Abs. 1 ThürDSG – begründet werden. Dies ergibt sich auch aus einer Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007, 1 BvR 2368/06 zur Videoüberwachung mit Aufzeichnung eines Kunstwerkes der Stadt Regensburg. Die Zulässigkeit von Videoüberwachung zur Wahrnehmung des öffentlich-rechtlichen Hausrechts ist inzwischen in § 25 a ThürDSG geregelt. Da dieser statthafte Beobachtungszweck aber nicht vorlag, konnte sich die Zulässigkeit der Videoüberwachung mangels einer gesetzlichen Befugnisnorm nur daraus ergeben, dass keine personenbezogenen Daten verarbeitet werden. Der TLfD stellte fest, dass durch die niedrige Qualität der Aufzeichnungen die Kfz-Kennzeichen und die Fahrzeuginsassen nicht zu identifizieren waren, Fahrzeugaufschriften waren je nach deren Größe aber noch erkennbar. Zwar gibt der Fahrzeughalter die Aufschriften auf seinem Fahrzeug freiwillig preis, dies gilt aber nicht unbedingt für den Fahrzeugführer. Im Übrigen kann allein durch die Wahrnehmung einer Videoanlage ein Überwachungsdruck bei den Betroffenen entstehen. Der TLfD hatte das Straßenbauamt aufgefordert, die Videoaufnahmen so zu erstellen, dass entweder die Fahrzeugauf-

schriften elektronisch unkenntlich gemacht werden oder aber die Videokameras auf die größtmögliche Unschärfe eingestellt werden. In einer Stellungnahme zur beschriebenen Problematik führt das TMBLV aus, zukünftig in diesen Bereichen auf den Einsatz von Videoüberwachung bei der Verkehrszählung zugunsten anderer geeigneter Erhebungsmethoden zu verzichten. Sollten doch Fälle auftreten, die die Videoüberwachung erforderlich machen, will sich das TMBLV zuvor an den TLfD wenden.

Der Einsatz von Videoüberwachung zu Zwecken der Verkehrsplanung, -zählung und -beobachtung ist auf der Basis der bestehenden Rechtsgrundlagen nicht zulässig, deshalb muss jeglicher Personenbezug vermieden werden.

13 Bildung, Wissenschaft, Forschung

13.1 Erhebungsbogen zur Vorschuluntersuchung

Eltern beschwerten sich beim TLfD darüber, dass auf dem Erhebungsbogen zur Einschuluntersuchung außer den Namen und Wohnanschriften von Mutter und Vater bzw. der Sorgeberechtigten auch deren Geburtsjahr und Beruf/Tätigkeit anzugeben war. Dies war umso überraschender, als die entsprechenden Formblätter für den Kinder- und Jugendärztlichen Dienst zur Schulärztlichen Vorsorgeuntersuchung bereits im Jahre 2003 geändert wurden. Nach § 3 Abs. 2 Thüringer Verordnung über die Schulgesundheitspflege (ThürSchulgespflVO) sind die Sorgeberechtigten verpflichtet, im Rahmen der Schuleingangsuntersuchung dem Schularzt Vorerkrankungen, bekannte Gesundheits- und Entwicklungsstörungen und den Impfstatus des Kindes mitzuteilen. Eine Erhebung des Berufs und des Geburtsdatums ist mit der genannten Regelung aber nicht zu vereinbaren und eine gesetzliche Auskunftspflicht hieraus nicht abzuleiten. Auf Nachfrage teilte das TMSFG dem TLfD mit, dass nach neueren Erkenntnissen ein Zusammenhang zwischen Sozialdaten und Gesundheitszustand bei Kindern bestehe und man somit besser in der Lage wäre, die Schulfähigkeit einzuschätzen und passenden Unterstützungsbedarf zu leisten. Das TMSFG hielt die Erhebung der Angaben des Berufs, der Tätigkeit und des Geburtsjahres des Sorgeberechtigten für entscheidend, sodass vorgeschlagen wurde, die entsprechenden Daten auf dem Erhebungsbogen als freiwillig zu kennzeichnen. Der TLfD hat auf der Grundlage von § 6 Abs. 1 Nr. 1 ThürSchulgespflVO, wonach auch die Beratung und Betreuung von Kindern und Jugendlichen mit sozialmedizinisch auffälligen Befunden gehört, die Auffassung des TMSFG geteilt und die Erhebung der o. g. Daten unter der Kennzeichnung als freiwillig zugestimmt.

Das Erheben von sozialmedizinischen Daten im Rahmen der Schuluntersuchung dient der Aufgabenerfüllung in der Schulgesundheitspflege. Die freiwillige Bekanntgabe solcher Daten durch die Sorgeberechtigten beachtet das Recht auf informationelle Selbstbestimmung der Betroffenen.

13.2 Braucht jede Schule einen Datenschutzbeauftragten?

Zwischen dem TLfD und dem TMBWK war strittig, ob die Aufgabe der von den staatlichen Schulen gemäß § 10 a Abs. 1 ThürDSG zu bestellenden Datenschutzbeauftragten durch die staatlichen Schulämter im jeweiligen Zuständigkeitsbereich wahrgenommen werden kann. Zwar konnte nach § 10 a Abs. 6 ThürDSG für mehrere Daten verarbeitende Stellen einer der Beschäftigten als gemeinsamer behördlicher Datenschutzbeauftragter bestellt werden, nach Auffassung des TLfD fiel hierunter aber nicht ein Beschäftigter aus einer übergeordneten Behörde, da eine solche Regelung ausdrücklich fehlte. Mit dem Gesetz zur Änderung des Thüringer Datenschutzgesetzes und anderer Vorschriften vom 30. November 2011 hat der Gesetzgeber speziell für diesen Fall eine Ergänzung in § 10 a Abs. 6 ThürDSG aufgenommen, wonach für die staatlichen Schulen die Aufsichtsbehörde einen ihrer Beschäftigten zum Beauftragten für den Datenschutz bestellen kann. Nach wie vor strittig ist, für welche Bereiche die in den staatlichen Schulämtern bestellten Beauftragten für den Datenschutz zuständig sind. Nach Darstellung des TMBWK erstreckt sich der Zuständigkeitsbereich lediglich auf die datenschutzrechtlichen Belange des pädagogischen Personals. Alle anderen Bereiche würden hingegen in den Zuständigkeitsbereich des Schulträgers fallen. Für den TLfD ergibt sich aus dem vom Schulträger finanziell zu tragenden Schulaufwand nicht, dass dieser auch die datenschutzrechtliche Verantwortung für alle Bereiche außerhalb des pädagogischen Personals zu übernehmen hat. So liegt es in der Entscheidung der Schulaufsichtsbehörde, ob und wenn ja, welche Verfahren zur automatisierten Verarbeitung personenbezogener Schüler-, Lehrer- und Elterndaten in der Schule zum Einsatz kommen. Weitere Beispiele sind die Verantwortung für den Betrieb von schuleigenen Homepages und die Administrierung der Schulsoft- und Hardware. Dies ergibt sich aus den Aufgaben und Befugnissen der Schulaufsichtsbehörden nach dem Thüringer Gesetz über die Schulaufsicht. Der TLfD wird weiterhin darauf drängen, dass die Sicherstellung des Datenschutzes in den staatlichen Schulen von den Schulaufsichtsbehörden übernommen wird.

Aufgrund des geänderten ThürDSG kann die Aufsichtsbehörde für die staatlichen Schulen einen ihrer Beschäftigten zum Beauftragten für den Datenschutz bestellen. Dieser hat die staatlichen Schulen bei

der Ausführung dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz zu unterstützen und auf deren Einhaltung hinzuweisen.

13.3 Datensparsamkeit bei Berufswahlveranstaltungen mit Schülern

Die Eltern eines Schülers beschwerten sich über die in den Thüringer Schulen umgesetzte Konzeption zur Berufsorientierung. Grundlage für die Berufswahlvorbereitung der Schüler ist der sogenannte Thüringer Berufswahlpass. Dieser wird seit dem Schuljahr 2004/2005 allen Schülern in der Klassenstufe 7 als Unterrichtsmaterial übergeben. Der Berufswahlpass soll den Schülern als Entscheidungshilfe bei der Berufswahl dienen und enthält neben zahlreichen Informationen und Hinweisen auch verschiedene Arbeitsblätter, mit deren Hilfe jeder Schüler schrittweise sein persönliches Profil bestimmen soll. Das Herausarbeiten des persönlichen Profils geht notwendigerweise einher mit der Verarbeitung von personenbezogenen Daten der Schüler. Solange der Berufswahlpass in der alleinigen Verfügungsgewalt des Schülers bzw. seiner Sorgeberechtigten liegt, bestehen keine datenschutzrechtlichen Bedenken. Allerdings wird der Schüler dazu angeregt, seinen persönlich erarbeiteten Berufspass Lehrern, Beratungskräften der Agenturen für Arbeit sowie Unternehmen im Bewerbungsverfahren vorzulegen. Somit werden personenbezogene Daten des Schülers Dritten bekannt. Insbesondere werden Unternehmen in einem Bewerbungsverfahren den Betroffenen um die Vorlage des Berufspasses ersuchen. Dem Bewerber steht es natürlich frei, in diese Unterlagen Einsicht zu gewähren. Allerdings kann dann beim Bewerber die Befürchtung entstehen, dass ihm bei einer Verweigerung der Vorlage des Passes möglicherweise Nachteile entstehen. Deshalb ist den Betroffenen aus datenschutzrechtlicher Sicht dringend zu raten, bereits beim Ausfüllen des Berufspasses darüber nachzudenken, welche personenbezogenen Daten ggf. Dritte erfahren sollen. Der TLfD bat bei einer Neuauflage des Berufswahlpasses um eine Überarbeitung der Unterlagen dahingehend, dass Schüler und Eltern für eine informierte Einwilligung besser über das Verfahren aufgeklärt werden. Inzwischen ist für das Schuljahr 2011/2012 die 8. Auflage des Thüringer Berufspasses erschienen, wobei der TLfD allerdings keine Gelegenheit erhielt, hierzu im Vorfeld Stellung zu nehmen. Das

Verfahren wird einer erneuten datenschutzrechtlichen Prüfung unterzogen werden.

Der TLfD hatte auch die Durchführung von Veranstaltungen zur Berufsorientierung bei einem Bildungsträger geprüft. Die Schüler erhalten dort individuelle Einschätzungen zu deren beruflichen Stärken und Entwicklungspotentialen. Der TLfD hat gegenüber dem Bildungsträger und dem zuständigen staatlichen Schulamt gefordert, vor Kursbeginn die Eltern und die Schüler schriftlich in dieses Verfahren einwilligen zu lassen. Ohne eine solche Einwilligung muss der Schüler zwar an dieser Schulveranstaltung teilnehmen, die Erstellung eines Persönlichkeitsprofils des Schülers durch den Bildungsträger darf dann aber nicht erfolgen.

Die Grenze, welche personenbezogenen Daten zur Erfüllung des gesetzlichen Bildungs- und Erziehungsauftrag der Schule bei den Schülern erhoben werden dürfen, ist fließend. Sobald keine Verpflichtung besteht, erforderliche Angaben zu machen, sind die Betroffenen umfassend auf die Freiwilligkeit ihrer Angaben hinzuweisen.

13.4 Verkehrssicherheitsforschungsvorhaben RETISS

Der TLfD wurde um seine datenschutzrechtliche Beurteilung des Demonstrationsprojekts „RETISS“ (Real Time Security Management System für Infrastrukturen) gebeten, an welchem das TLBV zur Erhöhung der Verkehrssicherheit des Tunnels „Rennsteig“ teilnimmt. Es handelt sich dabei um einen Bestandteil des Sicherheitsforschungsprogramms der Bundesregierung „Forschung für zivile Sicherheit“. Das Vorhaben wird aus Mitteln des Bundes finanziert. Neben der aus datenschutzrechtlicher Sicht unproblematischen Bestimmung von Fahrzeuganzahl, -geschwindigkeit und -abstand von in den Rennsteigtunnel einfahrenden Fahrzeugen durch in die Fahrbahn eingelassene Induktionsschleifen sollen alle Fahrzeuge mit einer Infrarotdetektion auf die insbesondere im Motor und an den Bremsen herrschenden Temperaturen in Echtzeit überprüft werden. Die während des Vorbeifahrens erstellten Infrarotbilder werden in einer Musterdatenbank für Fahrzeugdaten abgeglichen. Überschreiten die gemessenen Werte die für den jeweiligen Fahrzeugtyp maximal zulässigen Temperaturen an dem Bauteil, schlägt

das System Alarm. Diese Messungen werden etwa zwei Kilometer vor der Tunneleinfahrt mit an einer Schilderbrücke installierten Infrarotkameras durchgeführt. Perspektivisch ist vorgesehen, dass die Tunneleinfahrt im Gefahrenfall für den Verkehr gesperrt wird. Die Erforderlichkeit der Überwachung ergibt sich nach Angaben des TLBV aus mehreren Vorfällen im Jahr, bei denen Fahrzeuge brennend in einen Tunnel einfahren und immer die Gefahr besteht, dass eine Katastrophe ausgelöst wird. Bis zum Zeitpunkt des Gefahren Eintritts werden mit dem System weder Fahrzeuginsassen noch das Kfz-Kennzeichen oder Fahrzeugaufschriften festgestellt. Wird ein Fahrzeug vom System als überhitzt festgestellt, soll dieses dann identifiziert werden, um geeignete Maßnahmen zur Gefahrenabwehr noch vor Einfahrt des betroffenen Fahrzeugs in den Tunnel zu ergreifen. Zu diesem Zweck sind an der Schilderbrücke zusätzlich noch zwei Videokameras installiert, die im Fall einer Alarmauslösung des Systems ein Videobild des Fahrzeugs aufzeichnen. Die datenschutzrechtliche Problematik ergibt sich daraus, dass keine Rechtsgrundlage die grundsätzlich mit dem Einsatz einer Videoüberwachung verbundene Erhebung personenbezogener Daten für die vorliegenden Zwecke erlaubt. Der TLfD hat deshalb gegenüber dem TLBV gefordert, die Anlage technisch so zu gestalten, dass erst in dem Moment, in dem die Messeinrichtung kritische Temperaturen an einem Fahrzeug feststellt, ein das Fahrzeug identifizierendes Foto bzw. eine Videoaufnahme ausgelöst wird, ohne dass personenbezogene oder personenbeziehbare Daten verarbeitet werden. Da die Aufnahme des Fahrzeugs seitlich erfolgt, sind die Insassen und das Kfz-Kennzeichen nicht sichtbar. Andere lesbare Kennzeichen und Aufdrucke der Fahrzeuge sollen mit einem technischen Verfahren unkenntlich gemacht werden. Der Nachweis für die Funktionsfähigkeit dieses Verfahrens konnte aber bislang nicht erbracht werden. Da die Messanlage den Eindruck bei den Verkehrsteilnehmern erwecken kann, dass an dieser Stelle eine Videoüberwachung erfolgt, hat der TLfD vorgeschlagen, durch einen geeigneten Hinweis an der Schilderbrücke über den Zweck der Anlage zu informieren. RETISS befindet sich aktuell weiterhin in der Testphase. Eine vom TLBV zunächst angekündigte Pressekonferenz zur Vorstellung der Technik entfiel, da bisher nicht genügend Ergebnisse vorliegen. Der TLfD wird die weitere Entwicklung des Verfahrens begleiten.

Der Einsatz von Verkehrsüberwachungssystemen mit Videotechnik ohne Rechtsgrundlage ist nur zulässig, wenn die Verarbeitung von personenbezogenen Daten durch das Ergreifen geeigneter Maßnahmen ausgeschlossen ist.

13.5 Sicherheitsforschung muss Folgen für Persönlichkeitsrechte im Blick behalten

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die das Ziel haben, mithilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – möglichst frühzeitig bestimmte Verhaltensweisen in der Öffentlichkeit festzustellen, um „Gefährder“ zu entdecken. Ausgangspunkt ist ein Forschungsprogramm der EU (INDECT), mit dem Sicherheitsforschungen gefördert werden. Im Rahmen dieses Programms wird auch die Möglichkeit der Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts und vorwärtsgerichteter Videodatenströme durch die TU Ilmenau erforscht. Hierzu wurde eine Zusammenarbeit mit dem Flughafen Erfurt-Weimar vereinbart und der TlFD um datenschutzrechtliche Prüfung gebeten. Vorgesehen ist, dass zu besucherschwachen Zeiten mit Statisten der TU Ilmenau typische Wege von Reisenden auf dem Flughafen mittels Videoaufzeichnungen verfolgt und „vorausgesagt“ werden sollen. Durch die Videoaufzeichnungen werden personenbezogene Daten erhoben und genutzt. Hierfür muss es entweder eine gesetzliche Grundlage oder eine vorherige Einwilligung der Betroffenen geben, § 4 Abs. 1 ThürDSG. Die vorab erteilte Einwilligung der Betroffenen nach § 4 Abs. 2 ThürDSG ist zwingende Voraussetzung für die Zulässigkeit der beabsichtigten Datenerhebung und -nutzung, da eine andere gesetzliche Ermächtigungsgrundlage bislang nicht existiert. Das Forschungsvorhaben am Flughafen Erfurt-Weimar ist nach Ansicht des TlFD zulässig, wenn die Mitarbeiter des Flughafens und die Inhaber der dort angesiedelten Geschäfte vorab über die geplanten Aufnahmezeiten informiert werden. Während der Filmaufnahmen muss außerdem durch geeignete Hinweise über das Stattfinden der Filmaufnahmen und ihren Zweck sowie die Tatsache informiert werden, dass Aufnahmen von nicht am Projekt beteiligten Personen, die unbeabsichtigt aufgenommen wurden, entweder gelöscht oder durch Verpixelung unkenntlich gemacht werden. Gleichzeitig muss zur Zeit der Filmaufnahmen für betroffe-

ne Dritte ein Ansprechpartner zur Verfügung stehen, der über den Zweck des Projekts sowie über den Umgang mit Aufnahmen Unbeteiligter Auskunft geben kann. Unter diesen Voraussetzungen ist die Verarbeitung der personenbezogenen Daten, zu der auch die Erhebung zählt (§ 3 Abs. 3 Nr. 1 ThürDSG), sowie die Nutzung dieser Daten zulässig, da die Betroffenen eingewilligt haben, § 4 Abs. 1 ThürDSG. Die zufällig mit erfassten personenbezogenen Daten von unbeteiligten Personen werden nicht zielgerichtet erhoben und es ist durch die vorgesehene Löschung oder das Unkenntlichmachen dieser Daten sichergestellt, dass eine Nutzung dieser Daten ausgeschlossen ist. Bislang hat sich die Durchführung des Vorhabens aus technischen Gründen verzögert. Der TLfD hat sich vorbehalten, die konkrete Durchführung vor Ort zu kontrollieren.

Auch wenn im Rahmen der Forschung personenbezogene Daten erhoben und genutzt werden, kann dies datenschutzgerecht nur auf einer gesetzlichen Grundlage geschehen oder es muss eine Einwilligung des Betroffenen vorliegen. Der TLfD wird das Forschungsvorhaben weiter in datenschutzrechtlicher Hinsicht begleiten.

14 Entwicklungen der automatisierten Datenverarbeitung

14.1 Cloud-Computing

Zur datenschutzkonformen Gestaltung und Nutzung von Cloud-Computing hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine EntschlieÙung gefasst (Anlage 24), in der eine Orientierungshilfe zustimmend zur Kenntnis genommen wurde. Die Orientierungshilfe stellt den derzeit bekannten Stand zum Thema dar und verweist auf die Risiken des Cloud Computing und auf die nicht vollständig gesicherten rechtlichen Verhältnisse hin. Die Hauptverantwortung für die Daten verbleibt beim jeweiligen Anwender. Er muss entscheiden, ob er in Abwägung des Einsparungspotentials an eigenen Aufwendungen für Technik und Software mit den Risiken der jeweiligen Cloud einen Vertrag eingehen will oder nicht. Fraglich ist dabei, ob er die Risiken ausreichend erkennen kann und ob Anbieter von Cloud-Services überhaupt ernst zu nehmende Garantien geben. Entscheidet sich eine Stelle Thüringens für die Inanspruchnahme von Cloud-Services, so ist sie Cloud-Anwender. Handelt es sich bei der Stelle um eine öffentliche Stelle, so ist der Cloud-Anbieter Auftragnehmer nach § 8 ThürDSG. Nimmt diese öffentliche Stelle am Wettbewerb teil, so ist der Cloud-Anbieter, wie bei nicht-öffentlichen Stellen Auftragnehmer gemäß § 11 Abs. 2 BDSG. Der Cloud-Anwender bleibt sowohl nach § 8 Abs. 1 ThürDSG als auch nach § 11 Abs. 1 BDSG für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Da die Cloud keine geographischen Grenzen kennt und die stattfindende Datenverarbeitung gerade nicht ortsgebunden ist, muss für eine datenschutzrechtliche Betrachtung insbesondere über sämtlich mögliche Verarbeitungsorte informiert werden, da das geltende Datenschutzrecht an den Ort der Verarbeitung gebunden ist. Die damit bestehende Rechtsunsicherheit wird auch dadurch verstärkt, dass z. B. US-Behörden unter Berufung auf den Patriot Act auf alle Daten, die dort ansässige Firmen speichern, zugreifen können. Dies gilt auch für Daten europäischer Firmen, die etwa in Cloud-

Rechenzentren von Amazon oder Microsoft abgelegt sind. EU-Recht ist immer bereits dann anwendbar, wenn der Cloud-Anwender als verantwortliche Stelle im Rahmen der Tätigkeiten einer in der EU gelegenen Niederlassung personenbezogene Daten verarbeitet oder wenn die für die Verarbeitung verwendeten Mittel im Hoheitsgebiet der EU gelegen sind. Aufgrund des innerhalb des Europäischen Wirtschaftsraums (EWR) weitgehend harmonisierten Datenschutzniveaus gelten für alle Cloud-Anwender, Cloud-Anbieter und Unter-Anbieter dieselben datenschutzrechtlichen Anforderungen nach der Richtlinie 95/46/EG.

Erfolgen die Datenverarbeitungen allerdings außerhalb der EU und des EWR, indem die Cloud-Anbieter und/oder Unter-Anbieter eine Datenverarbeitung in Drittstaaten vornehmen, so gelten zudem die besonderen Anforderungen gemäß § 23 ThürDSG bzw. §§ 4 b, 4 c BDSG für den Drittstaatentransfer. Falls in dem Drittstaat kein angemessenes Datenschutzniveau besteht, müssen daher durch den Cloud-Anwender als verantwortliche Stelle ausreichende Garantien zum Schutz des allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorgewiesen werden. Die Garantien können sich aus Vertragsklauseln oder auch aus Binding Corporate Rules ergeben. In jedem Fall ist ein besonderes Augenmerk auf die vertragliche Festlegung eines technischen und organisatorischen Datenschutzes entsprechend § 8 Abs. 2 ThürDSG bzw. § 11 Abs. 2 BDSG zu legen. Ebenso wenig entbindet z. B. eine bloße Safe-Harbor-Zertifizierung den Cloud-Anwender von seiner Kontrollpflicht analog § 8 Abs. 2 ThürDSG bzw. § 11 Abs. 2 Satz 3 BDSG.

Länderübergreifende gesetzliche Regelungen außerhalb der EU in Bezug auf das Datenschutzrecht gibt es noch nicht und sie sind auch nur schwer gestaltbar, d. h. alle öffentlichen Stellen, die mit zu schützenden personenbezogenen Daten arbeiten, können länderübergreifende Cloud-Angebote gegenwärtig nicht nutzen. Deshalb wird im öffentlichen Bereich zunächst noch die Private- bzw. Community-Cloud der sicherste Weg sein, um virtuelle Server an von mehreren Behörden gemeinsam genutzten Standorten zu hosten. Die Orientierungshilfe ist abrufbar unter:

www.thueringen.de/datenschutz/veroeffentlichungen/orientierungshilfen

Cloud-Anbieter müssen ihre Leistungen datenschutzkonform gestalten, d. h. sie müssen detaillierte und transparente Informationen über die technischen, organisatorischen und rechtlichen Rahmenbedingungen einschließlich eines Sicherheitskonzeptes bereitstellen.

Eine entsprechende vertragliche Regelung muss Aussagen zum Ort der Datenverarbeitung sowie eine Benachrichtigung bei einem Ortswechsel, erforderlichenfalls Anforderungen zur Portabilität bzw. Interoperabilität beinhalten. Nach Möglichkeit sind Sicherheits- und Datenschutzmaßnahmen zwischen Anbieter und Anwender abzustimmen. Aktuelle und aussagekräftige Nachweise (z. B. Zertifikate unabhängiger Prüfungsorganisationen), die Informationssicherheit betreffend, stärken das Vertrauen der Cloud-Anwender.

Cloud-Anwender dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie sich in die Lage versetzt sehen, ihre Pflichten als verantwortliche Stelle in vollem Umfange wahrzunehmen und die vorhandenen Datenschutz- und Informationssicherheitsanforderungen gemäß § 8 ThürDSG bzw. § 11 BDSG geprüft haben. So lange hier Zweifel bestehen, sollte auf Cloud-Computing verzichtet werden.

14.2 RFID-Selbstregulierung funktioniert nicht

Seit dem 12. Mai 2009 liegt eine „Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“ vor (2009/387EG). Alle Mitgliedstaaten waren aufgefordert, spätestens 24 Monate nach der Veröffentlichung dieser Empfehlung mitzuteilen, welche Maßnahmen sie eingeleitet haben, um dieser Empfehlung nachzukommen. Die Kommission selbst beabsichtigt drei Jahre nach der Veröffentlichung einen Bericht über die Umsetzung dieser Empfehlung, ihre Wirksamkeit und ihre Auswirkungen auf die Wirtschaftsteilnehmer und Verbraucher vorzulegen. Im Februar 2011, also drei Monate vor Fristende, forderte der Bundesrat die Bundesregierung auf, die Empfehlung der EU-Kommission auf nationaler Ebene umzusetzen und zu konkretisieren. So wurde von der Bundesregierung erwartet, dass sie sich bei den Verhandlungen mit der Wirtschaft für Verbraucherinformation und Datenschutzkonzepte und für die Kennzeichnung und Deaktivierungsmöglichkeit der RFID-Chips in verbraucherrelevanten Bereichen einsetzt. Wenn die

Selbstverpflichtung der Wirtschaft nicht gelingt, sollte eine gesetzliche Regelung angestrebt werden (BR-Drs. 48/11).

Bislang hat nur das BSI, basierend auf der BSI-Richtlinienreihe TR 03126 (TR RFID), einen Leitfaden veröffentlicht, durch den die deutsche Industrie bei der Erstellung eines Privacy Impact Assessments (Datenschutzfolgeabschätzung) – entsprechend der EU-Empfehlung – unterstützt werden soll. In der TR RFID selbst wurden Details zu folgenden Verfahren veröffentlicht:

- „eTicketing für Veranstaltungen“,
- „eTicketing in öffentlichen Personenverkehr“,
- „Near Field Communication (NFC)-basierte eTicketing“,
- „Handelslogistik“ und
- „elektronischer Mitarbeiterausweis“

Diese Dokumente stehen auch zum Download zur Verfügung (https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03126/index_htm.html).

Auch im Kreis der Datenschutzbeauftragten des Bundes und der Länder wird die fehlende Umsetzung der Empfehlung der EU-Kommission derzeit kritisch diskutiert, da die Leitlinie und die TR RFID nicht die Selbstverpflichtung der Wirtschaft und die zu ergreifenden Maßnahmen durch die Bundesregierung ersetzen können. Zudem ist nicht nur der datenschutzgerechte Einsatz von RFID in Deutschland gefährdet, sondern auch auf den Bericht der Kommission ist eine positive Einflussnahme verwirkt worden. Da für Anfang 2012 eine neue EU-Verordnung zum Datenschutz angekündigt wurde, ist zu erwarten, dass sich die Konferenz der Datenschutzbeauftragten auf ihrer Frühjahrskonferenz noch einmal mit dieser Thematik befassen wird.

Nicht nur der Bundesrat, sondern auch die Datenschutzbeauftragten des Bundes und der Länder erwarten von der Bundesregierung die Umsetzung der Empfehlung der EU-Kommission hinsichtlich des datenschutzgerechten Einsatzes von RFID.

14.3 Sicheres Löschen von Festplatten

Eine Orientierungshilfe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten mit letztem Stand vom 7. Oktober 2004

gab bisher Hinweise für das Verfahren zum sicheren Löschen von Festplatten. Danach ist sowohl aus Sicht des Datenschutzes als auch der IT-Sicherheit beim Löschen von sensiblen oder vertraulichen Daten auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu nicht aus, da eine Rekonstruktion der Daten mit frei verfügbaren Softwarewerkzeugen immer noch möglich ist. Daten, die sicher gelöscht werden sollen, müssen durch physikalische Maßnahmen (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder durch mehrmaliges Überschreiben unkenntlich gemacht werden. Der Arbeitskreis Technik plant die Orientierungshilfe zu überarbeiten.

Als Werkzeug zum Überschreiben von Datenträgern kam bisher die vom BSI entwickelte Software VS-Clean zum Einsatz. Inzwischen wurde, nach Angaben des BSI, der Vertrieb von VS-Clean (zuletzt Version 2.1, Stand 2002) eingestellt. Eine Weiterentwicklung von VS-Clean ist nicht vorgesehen. Für den Einsatz im Geheimschutz befindet sich ein neues Produkt im Zulassungsverfahren (www.bsi.bund.de). Da es noch kein Produkt gibt, das den überarbeiteten Anforderungen des BSI vollständig entspricht, ist momentan noch keine abschließende Produktempfehlung möglich.

Seit August 2011 steht ein neues Hinweisblatt des BSI zum Überschreiben von Festplatten zum Download zur Verfügung, dessen Inhalt auszugsweise im Folgenden dargestellt wird:

Die Entwicklung ständig größerer Festplattenkapazitäten ist mittlerweile im Terabyte-Bereich angekommen. Diese modernen Festplatten setzen vermehrt abweichende Sektorgrößen ein (z. B. vier Kilobyte anstelle von 512 Byte). Solche Festplatten müssen mit Software überschrieben werden, die diese Sektorgrößen berücksichtigt. Andernfalls wird die Festplatte nur zum Teil gelöscht und große Datenmengen wären wiederherstellbar. Durch die Software VS-Clean können Festplatten ab einer Kapazität von zwei Terabyte weder richtig erkannt noch vollständig gelöscht werden. S-ATA-, USB-Festplatten und RAID-Systeme werden von VS-Clean auch nicht unterstützt.

Moderne Festplatten bieten zudem die Möglichkeit, Bereiche für bestimmte Zwecke zu reservieren und damit für den normalen Zugriff zu sperren. Dies geschieht in Form von Techniken wie DCO (Device Configuration Overlay) oder HPA (Host Protected Area), die eine künstliche Beschränkung der Kapazität der Festplatte vornehmen und somit weite Bereiche der Festplatte, da nicht erkannt, ungelöscht belassen. Geeignete Lösch-Tools müssten diese Techniken erkennen und betroffene Bereiche auflösen, bevor mit dem Überschreiben begonnen werden kann.

Es wird auf das Risiko nicht gelöschter Speicherbereiche durch die von Festplatten interne Umorganisation altersschwacher Sektoren hingewiesen (sogenannte "bad blocks", "reallocated sectors"). Diese Sektoren können von außen nicht mehr unmittelbar angesprochen und damit auch nicht überschrieben werden. Festplatten mit permanentem Halbleiterspeicher (SSD/Flash-Technologie bzw. Hybrid-Festplatten) organisieren die Speicherung hochdynamisch und komplex, sodass wegen der internen Abläufe auch bei Anwendung üblicher Überschreibsoftware keine Löscharantie besteht. Bei diesen Technologien muss beim Löschen davon ausgegangen werden, dass große Bereiche der Nutzerdaten nicht erfasst werden und selbst bei mehrfacher Anwendung/Mehrfachüberschreiben immer noch eine große Menge an Nutzerdaten verbleiben kann, die nicht ein einziges Mal überschrieben wurden (vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Produkte/VSClean/Ueberschreiben_Festplatten.pdf).

Um einschätzen zu können, ob sich eine Software zum vollständigen Löschen einer Festplatte eignet, sollte sich der Anwender unbedingt davon überzeugen, dass alle in einem System verbauten Festplatten vom Löschprogramm mit der korrekten Kapazität (Sektoranzahl) erkannt werden.

Wenn ein Computer entsorgt werden soll, der Daten mit hohem Schutzbedarf enthält, sind dessen Festplatten physisch zu zerstören. Das gilt auch für Speichermedien wie CDs oder USB-Sticks. Bei defekten Festplatten, die nicht mehr überschrieben werden können, bleibt ebenfalls nur das physikalische Vernichten.

14.4 Cookies und Co

Cookies (Kekse) sind kleine Dateien mit Text-Informationen, die ein Web-Server an den Web-Browser der jeweiligen Arbeitsstation überträgt und dort auf der Festplatte speichert. Dabei wird ein Verfallsdatum vorgemerkt. Erreicht ein Cookie sein "Verfallsdatum", so wird es vom Browser gelöscht. Normale Cookies können nicht größer als vier Kilobytes sein, sie werden niemals vom Browser wie ein Programm ausgeführt. Demnach können sie auch keine Viren verbreiten. Die Cookie-Technik erlaubt es einem Webserver, auf dem PC des Anwenders Informationen zu hinterlegen. Da der Web-Server nicht direkt auf die Datenträger der Anwenders Zugriff hat, muss er hierfür den Browser benutzen. Dieser kann aber nur das speichern, was er ohnehin schon kennt (z. B. die aktuelle IP-Adresse, die URL, Rechnernamen, Domain, Grafikeinstellungen, Betriebssystem, ggf. Anwendereingaben). Beim nächsten Aufruf derselben Webseite werden die zuvor gespeicherten Daten aus der Cookie-Datei automatisch wieder an den Web-Server übertragen. Cookies können jedoch nicht nur von Webseiten gesetzt werden, sondern auch bei jedem anderen http-Zugriff in das Internet. Hierunter fallen auch Inhalte, die beim Betrachten einer E-Mail oder eines Dokuments aus dem Internet geladen werden, wobei dies oft unsichtbar für den Benutzer geschieht (sogenannte Webbugs).

Vorteil der Cookie-Technik ist, dass bei einem wiederholten Aufruf einer bereits bekannten WebSite vorab getätigte Einstellungen des Nutzers (z. B. E-Mail-Adresse, Benutzername, Themenschwerpunkte, Sprachen, Menüs, Kundendaten u. a.) nicht ständig erneut eingegeben bzw. ausgewählt werden müssen (Wiedererkennungseffekt).

Nachteil oder Gefahr

Es können mehrere Internet-Anbieter gemeinsam Cookies auf dem Browser des Benutzers verwalten, wenn sie ihre Seiten miteinander verkettet haben (z. B. durch Werbebanner). Auf diese Weise wird es möglich, das Surfverhalten innerhalb dieses Zusammenschlusses zu ermitteln, da die gleichen Cookies dann auch von den verknüpften Seiten gelesen werden können. Diesen Trick nennt man **Webbug**. Er ermöglicht es, den Weg eines Surfers durch das Internet zu verfolgen, und somit ein gezieltes Tracking durchzuführen. Diese „Webbugs“ werden oft als sehr kleine Pixelgrafiken (es genügt ein

einziges Pixel) auf andere Webseiten gelegt und auch dazu verwendet, die Aufrufhäufigkeit bestimmter Webseiten zu ermitteln.

Richtig gefährlich wird es, wenn auf der Seite eines Anbieters ein Formular mit Namen, Anschrift und weiteren sensiblen Daten abgesendet wird, denn dann ist nicht nur das Surfverhalten bekannt, sondern auch die Person, die dieses Surfverhalten an den Tag gelegt hat, ggf. sogar deren Kreditkartennummer und weitere sensible Daten (z. B. Login). Ein wiederverwendbares Profil wurde geschaffen, das so lange erhalten bleibt, wie das betreffende Cookie gültig ist, also möglicherweise über Jahre hinweg, wenn es nicht manuell gelöscht wird. Es besteht sogar die Gefahr, dass mit nur einem Mausklick wiederholt Aktionen ausgeführt werden könnten (z. B. Bestellungen), die dann bspw. dazu führen, dass ohne eine weitere Bestätigung ein Geldbetrag von einer Kreditkarte abgebucht wird.

Ohne Cookie-Spezial-Tool ist es daher sinnvoll, im Normalfall Cookies im Browser zu deaktivieren und nur auf Seiten von vertrauenswürdigen Anbietern (zum Beispiel um einen Warenkorb zu verwalten) vorübergehend aktiviert zu belassen. Sind Cookies aktiviert, sollte bei Dateneingaben in Formularen besonders vorsichtig vorgegangen werden. Löscht man hingegen Cookies regelmäßig, werden derartige Gefahren ausgeschlossen. In den meisten Browsern ist es möglich, "normale" browserkompatible Cookies zu unterdrücken oder zu löschen.

Benutzerwiedererkennung über IP-Adresse

Viele Internet-Provider arbeiten mit "dynamischen IP-Adressen". Das bedeutet, dass man bei jeder Internet-Verbindung eine neue Adresse erhält. Die IP-Adresse wird benötigt, um einen Rechner im Internet zu identifizieren. Der Server weiß nun, an welche Adresse er die angeforderten Daten schicken soll, weiß aber nicht wirklich, welche Person sich hinter dieser IP-Adresse verbirgt. Nun kann aber der Server ein Cookie an den Browser übertragen, das eine eindeutige "Benutzerkennung" enthält und dieses mit einer langen Lebensdauer versehen. Das Cookie würde nach Beendigung des Browsers in der entsprechenden Datei gespeichert verbleiben. Somit wird der Benutzer von diesem Server auch beim nächsten Besuch eindeutig zu identifizieren sein, obwohl er diesmal vielleicht eine andere IP-Adresse erhalten hat.

Neuere Cookie-Technologien, die sich nicht unmittelbar über Browsereinstellungen steuern lassen, sind z. B. sogenannte **Flash-Cookies**. Hierzu hat das ULD Schleswig-Holstein im 32. Tätigkeitsbericht (Nr. 10.4) auf folgendes hingewiesen:

„Der Browserzusatz Flash der Firma Adobe ist nach Angaben des Herstellers auf über 90 % aller PCs installiert und sorgt für die Darstellung von Animationen und Videosequenzen. Zum Speichern von Parametern dient dem Flash-Plugin ein eigenes Speichersystem, die Local Shared Objects (LSO). Diese Dateien können vom Flash-Plugin auf dem Nutzerrechner abgelegt werden. Über den Browser hat der Nutzer darauf jedoch keinen Zugriff, sodass auf vielen Rechnern diese Flash-Cookies unentdeckt bleiben. Hinzu kommt, dass dasselbe Flash-Cookie für alle auf dem System befindlichen Browser gilt. Wie normale Cookies können Flash-Cookies durchaus sinnvoll sein. Verbreitet ist z. B. das Speichern von Spielständen bei Flash-basierten Online-Spielen. Aber auch banale Dinge wie die Lautstärkeinstellungen von YouTube-Videos werden mithilfe der Local Shared Objects gespeichert. Löschen lassen sich diese Flash-basierten Cookies nur über Adobes Webseiten. Die dafür einschlägige Internetadresse lautet:

www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html

Ähnliche Speichermodelle wie Adobe Flash stellen auch ‚Microsoft Silverlight‘ und ‚Java‘ von Sun bereit. Auch hier sind die Einstellungen zum Deaktivieren von Cookie-ähnlichen Objekten nicht leicht auffindbar. Microsoft versteckt sein Konfigurationstool ‚Silverlight.Configuration.exe‘ im Verzeichnis C:\Programme\Microsoft Silverlight\... Die Java-Konfiguration javacpl.exe liegt bei solchen Rechnern standardmäßig im Verzeichnis C:\Programme\Java\[Version]\bin\.

Eine dritte Inkarnation der herkömmlichen Cookie-Idee stellt der sogenannte DOM-Storage-Mechanismus (DOM: Document Object Model) dar, der seit Firefox 2 in aktuellen Browsern zu finden ist. DOM Storage erweitert die klassische Cookie-Idee im Kern um eine flexiblere Adressbehandlung und vergrößert den verfügbaren Speicherplatz. Können klassische Cookies gerade mal 4 Kilobyte fassen,

kann ein DOM Storage Cookie deutlich mehr an Daten speichern, nämlich bis zu fünf Megabyte beim Firefox-Browser und sogar bis zu zehn Megabyte beim Internet Explorer. Der dahinterstehende Gedanke ist ironischerweise sogar datenschutzfördernd: Dienste wie Online-Textverarbeitungen können in solchen **Mega-Cookies** ihre Dokumente ablegen, sodass der Nutzer nicht mehr gezwungen ist, diese auf dem Server des Anbieters zu speichern. Trotzdem bleiben auch hier sämtliche Implikationen konventioneller Cookies in Bezug auf langfristige Verkettbarkeit bestehen. Zudem mangelt es bislang an Transparenz für den Nutzer. Obwohl solche Mega-Cookies vom Browser erzeugt werden und nicht von externen Programmen wie Flash, tauchen sie nicht in der browserinternen Übersicht der gespeicherten Cookies auf.“

In jedem der gängigen Browser gibt es eine "Cookie-Verwaltung", die ein Löschen bzw. Deaktivieren normaler Cookies ermöglicht. Die Vielfalt der möglichen Browsereinstellungen erreicht jedoch bei manchem Benutzer die Grenze der Zumutbarkeit im Umgang mit der Spezifik der veränderbaren Parameter. Deshalb gibt es neben dem manuellen Löschen spezielle, z. T. frei verfügbare Tools, mit denen eine bessere Cookie-Verwaltung möglich ist.

15 Technische Entwicklungen in der Thüringer Landesverwaltung

15.1 Kontrollen der DMS in den obersten Landesbehörden

Der Einsatz von Dokumentenmanagementsystemen (DMS) birgt neben Vorteilen, insbesondere Effektivitätssteigerungen bei der Vorgangsverwaltung in den öffentlichen Stellen, auch neue Risiken für das Grundrecht auf informationelle Selbstbestimmung. Mit einem DMS können „auf Knopfdruck“ durch Datenverknüpfungen aus einer komplexen Datensammlung völlig neue Informationen gewonnen werden. Wegen der durch den Einsatz von DMS bedingten elektronischen Abbildung sämtlicher Bearbeitungsschritte entstehen eine Vielzahl zusätzlicher Protokoll- und Verfahrensdaten im System, die mitarbeiterbezogen ausgewertet werden und zur Verhaltens- und Leistungskontrolle der Beschäftigten herangezogen werden könnten. Vor dem Einsatz von DMS müssen deshalb Anforderungen für datenschutzgerechte Lösungen formuliert und umgesetzt werden.

Der TLfD hat im Berichtszeitraum damit begonnen, den Einsatz von DMS insbesondere hinsichtlich der Verarbeitung sensibler personenbezogener Daten zunächst bei den obersten Landesbehörden zu überprüfen und diese vorerst um die für eine Sachstandsanalyse notwendigen Informationen sowie ggf. bei Nutzung eines DMS um die erforderlichen Dokumente (Sicherheitskonzept nach § 9 Abs. 2 ThürDSG, organisatorische Regelungen für das eingesetzte DMS, datenschutzrechtliche Freigabe nach § 34 ThürDSG, Formblatt zum Verfahrensverzeichnis nach § 10 ThürDSG, Dienstvereinbarungen mit dem Personalrat und ggf. weitere Regelungen und Festlegungen zum Umgang mit Personaldaten im Rahmen des DMS) gebeten.

Im Ergebnis der Mitteilungen ist z. B. im TMLFUN kein DMS im Einsatz und die Einführung eines derartigen Systems auch nicht geplant. Verschiedene Ressorts (z. B. TMBVL; TSK; TMBWK) nutzen das zum Einsatz kommende DMS zurzeit lediglich als Schriftgutverwaltungssystem, haben aber ggf. erste Überlegungen hinsichtlich eines weitergehenden Einsatzes getroffen.

Ein DMS mit unterschiedlicher Ausbaustufe haben das TMWAT, TMSFG, TIM, der TLT und das TFM. Im TFM wurde dem TLfD im

Rahmen einer Vor-Ort-Kontrolle das DMS vorgestellt. Die Planung/Durchführung des Piloten „Einsatz VISkompakt“ wird nach Angaben der Gesprächspartner im TFM zurzeit mit ca. 30 Personen getestet und soll zum Jahresende 2012 ausgerollt werden.

Der Einsatz eines DMS wirkt sich innerhalb der öffentlichen Stelle auf die Organisationseinheiten unterschiedlich aus, sodass der TLfD unbedingt eine frühe Beteiligung des IT-Sicherheitsbeauftragten, des behördlichen Datenschutzbeauftragten, der Personalvertretung, der Verantwortlichen der betroffenen Fachverfahren, der Poststelle, der Registratur und der Mitarbeiter des IT Bereiches empfiehlt.

Vor dem Einsatz von Dokumentenmanagementsystemen sind u. a. die notwendigen technisch-organisatorischen Maßnahmen gemäß § 9 ThürDSG zur Gewährleistung des informationellen Selbstbestimmungsrechts des Einzelnen zu treffen

Anlage 1

EntschlieÙung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Effektiver Datenschutz braucht unabhängige Datenschutzkontrollen!

1. Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Artikel 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten. Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.

-
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
 - Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
 - Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
 - Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Entschließung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Ein modernes Datenschutzrecht für das 21. Jahrhundert

Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und

Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

Anlage 3

Entschliebung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Entschließung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Körperscanner - viele offene Fragen

Der Anschlagversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagversuchs von Detroit verwendet worden sind.
2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.
3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürfen z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Entschließung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein

unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
- die Leistung, Wirkung sowie der Erfolg und die Effizienz,
- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsöffener Prozess, der einer ständigen Optimierung bedarf.

Entschließung

der 79. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 17./18. März 2010 in Stuttgart

Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1 b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder

öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

Entschließung zwischen den Konferenzen 2010

Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz (Umlaufentschließung vom 11. Oktober 2010)

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen.

Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages - RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,
- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und 2
- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

Entschließung zwischen den Konferenzen 2010

Erweiterung der Steuerdatenbank enthält große Risiken

(Umlaufentschließung vom 24. Juni 2010)

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer
Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat
In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs
Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept
Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein

Anlage 9

Entschließung zwischen den Konferenzen 2010**Beschäftigtendatenschutz stärken statt abbauen**

(Umlaufentschließung vom 22. Juni 2010)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigten-datenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.
- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln - etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.
- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn - wie im Entwurf vorgesehen - Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Be-

schäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv - und nicht erst auf Nachfrage - darüber aufzuklären, woher die verwendeten Daten stammen.

- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.
- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Anlage 10

Entschließung

der 80. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 03./04. November 2010 in Freiburg

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung

wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die - ggf. gänzlich unverdächtigen - Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

Entschließung

der 80. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 3./4. November 2010 in Freiburg

Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen.

Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

Anlage 12

EntschlieÙung

der 80. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 03./04. November 2010 in Freiburg

Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mithilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Entschließung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90 / DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
 - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
 - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
 - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.
- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.
- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.
- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
 - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
 - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.
- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemäßregelt zu werden.
- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

-
- zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
 - zur privaten Nutzung von Telekommunikationsdiensten,
 - zum Thema Whistleblowing,
 - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
 - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
 - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Anlage 14

Entschließung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

**Mindestanforderungen an den technischen Datenschutz
bei der Anbindung von Praxis-EDV-Systemen an medizinische
Netze**

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe <http://www.kbv.de/rechtsquellen/24631.html>).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.
7. Grundstandards – wie beispielsweise die Revisionsicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

- a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

- b) - eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Entschließung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit - auch für die Strafverfolgungsbehörden - zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter

strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

Entschließung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen auffindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

Entschließung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

**Gravierende Defizite bei der Umsetzung des
SWIFT-Abkommens - dringender
Handlungsbedarf auf nationaler und europäischer Ebene**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass - wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat¹ Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (<http://europoljsb.consilium.europa.eu/about.aspx>) abrufbar.

1 - EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beach-

¹ Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (<http://europoljsb.consilium.europa.eu/about.aspx>) abrufbar.

tung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

EntschlieÙung

der 81. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 16./17. März 2011 in Würzburg

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankengesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

Anlage 19

Entschließung zwischen den Konferenzen 2011**Funkzellenabfrage muss eingeschränkt werden!**

(Umlaufentschließung/27. Juli 2011)

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100 g Abs. 2 Satz 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Artikel 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100 a StPO – gegen bestimmte einzelne Tatverdächtige. Sie

offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

Anlage 20

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir“-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungstechnik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profildaten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Anlage 21

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertbezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfang sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlssysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbezogene Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

**Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne
Überblick**

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

Datenschutzkonforme Gestaltung und Nutzung von Cloud- Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragerfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe¹ der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

¹ http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Anlage 25

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

**Einführung von IPv6 steht bevor: Datenschutz ins Netz
einbauen!**

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IPAdresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mithilfe von Zusatzinformationen, die dem Betreiber eines Internet- Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internet- zugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (*privacy by design*) und dementsprechende Voreinstellungen wählen (*privacy by default*). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.
- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.
- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (*privacy by default*), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.
- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.
- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.
- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.
- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.
- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ *whois* aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des *whois*-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den *whois*-Dienst künftig als verteilte Datenbank gestaltet, sodass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

Entschließung

der 82. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. September 2011 in München

Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht während beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

Abkürzungsverzeichnis

Abkürz.	Bedeutung
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaften
AVBWasserV	Allgemeinen Bedingungen für die Versorgung mit Wasser
BDSG	Bundesdatenschutzgesetz
BfV	Bundesamt für Verfassungsschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfSchG	Bundesverfassungsschutzgesetz
BZRG	Bundeszentralregistergesetz
DMS	Dokumentenmanagementsystemen
ELStAM	elektronische Lohnsteuerabzugsmerkmale
EnWG	Energiewirtschaftsgesetz
ESTG	Einkommenssteuergesetz
EWR	Europäischen Wirtschaftsraums
EuGH	Europäischer Gerichtshof
GefTierG	Gesetzes zum Schutz der Bevölkerung vor gefährlichen Tieren
GewO	Gewerbeordnung
GKI	Gemeinsamen Kontrollinstanz
HAMASYS	Haushaltsmanagementsystem
HZD	Hessischen Zentrale für Datenverarbeitung
IGVP	Integrationsverfahren der Polizei
INPOL	Polizeilichen Informationssystem
MRRG	Melderechtsrahmengesetz
NADIS	nachrichtendienstliches Informationssystem
PAG	Polizeiaufgabengesetz
PStG	Personenstandsgesetz
RBStV-E	Rundfunkbeitragsstaatsvertrages
RETISS	Real Time Security Management System für Infrastrukturen
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
TerrorBekämpfungErgG	Terrorismusbekämpfungsgesetz

TFM	Thüringer Finanzministerium
ThürAbfG	Thüringer Abfallwirtschaftsgesetz
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürGemHV	Thüringer Gemeindehaushaltsverordnung
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKO	Thüringer Kommunalordnung
ThürMeldeG	Thüringer Meldegesetz
ThürMeldeVO	Thüringer Meldeverordnung
ThürRettG	Thüringer Rettungsdienstgesetz
ThürSchulG	Thüringer Schulgesetz
ThürSchulgespflVO	Thüringer Verordnung über die Schulgesundheitspflege
ThürStAnz	Thüringer Staatsanzeiger
ThürStatG	Thüringer Statistikgesetz
ThürUIG	Thüringer Umweltinformationsgesetz
ThürVerfSchG	Thüringer Verfassungsschutzgesetz
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TLBV	Thüringer Landesamt für Bau und Verkehr
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLKA	Thüringer Landeskriminalamt
TLS	Thüringer Landesamt für Statistik
TLT	Thüringer Landtag
TLVwA	Thüringer Landesverwaltungsamt
TMBLV	Thüringer Ministerium für Bau, Landesentwicklung und Verkehr
TMG	Telemediengesetz
TMLFUN	Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz
TMSFG	Thüringer Ministerium für Soziales, Familie und Gesundheit
TMWAT	Thüringer Ministerium für Wirtschaft,

ULD	Arbeit und Technologie Unabhängiges Landeszentrum für Daten- schutz Schleswig-Holstein
ZBS	Zentrale Bußgeldstelle
ZensG	Zensusgesetz

Sachregister

Abfallsatzung	11.4
Abrufverfahren	2.1, 9.1
Adressfeld	7.7
ALG II	11.7
Amtsarzt	6.2
Amtsblatt	5.2
Arbeitnehmer	6.4
Arbeitslosengeld II	11.6
Archivgut	5.13
ARGE	11.7; 11.8
Arzt	11.1; 11.9
Aufbewahrungsfrist	6.3
Auftragsdatenverarbeitung	4.1; 8.3
Beanstandung	5.1; 5.5; 5.8; 7.3; 7.4; 7.5; 7.7; 9.1; 10.2; 10.3
Beauftragter für den Datenschutz	13.2
Berufswahlpass	13.3
Beschäftigtendaten	6.1
Bildaufzeichnung	12.5
Bildschirmanzeige	9.3
Bildungspaket	11.6
Bundesmeldegesetz	5.9
Cloud Computing	14.1
Cookie	4.1
Datenabgleich	7.4
Datenschutznovelle	2.3
Datenübermittlung	9.1; 12.4
Dienstvereinbarung	6.4
Diskretionszone	9.3
Dokumentenmanagementsystem	15.1
Einkommensnachweis	5.6
Einwilligung	7.2; 7.3; 9.1; 12.1; 13.1; 13.3
elektronische Aufenthaltsüberwachung	10.4
EU-Datenschutzverordnung	3.1
Europol	3.3
Evaluierung	8.1
Festplatte	14.3

Flash-Cookie	14.4
Flugpassagierdaten	3.2
Fremdenverkehrsabgabe	5.8
Funkzellenabfrage	10.3
Gebührenabrechnung	5.7
Geldautomat	9.3
Gesundheitsdaten	11.9
Gewerberegister	12.4
GEZ	4.3
Grundbuchauszug	12.3
Grundschutzkatalog	5.1
Halterdaten	12.6
Hausrecht	5.5
Heads-Konzeption	10.4
Hundehalterregister	5.14
INPOL	7.5
Intelligente Stromzähler	12.2
Internet	2.3; 4.2 ;5.2; 12.1
Jobcenter	11.7; 11.8
Kita-Gebühren	5.6
Kommunalaufsicht	5.8
Kommunikationsüberwachung	10.3
Kontrollkompetenz des LfD	8.3; 10.2; 10.3
Konzerndatenschutz	6.1
Körperscanner	7.1
Kosten der Unterkunft	5.4
Krankenhaus	11.1; 11.9
Krankenkasse	11.3
Kundenadressen	5.4
Kurbeitrag	5.10
Löschung	5.6
magnetische Datenträger	14.3
medizinische Netze	11.9
Mega-Cookie	14.4
Melderegisterauskunft	5.11
Meldescheinverordnung	5.10
Menschenwürde	7.1
Mietspiegel	5.4
Mobilfunk	4.4
Modernisierung des Datenschutz-	2.1, 2.3; 3.1

rechts	
Mustererkennung	13.5
NADIS	8.2
Notruförtung	4.4
Offenbarungsbefugnis	6.2
Online-Petition	2.2
Patientendaten	11.1
Personalakten	6.1; 6.2, 6.3
Pflegestützpunkt	11.2
Pflegeversicherung	11.2; 11.3
Postlauf	5.3
Protokollierung	5.11; 7.5; 7.6
Quellen-TKÜ	10.2
RETISS	13.4
RFID	14.2
Rundfunkgebühren	4.3
Schularzt	11.5
Schuluntersuchungen	11.5; 13.1
Schulzahnarzt	11.5
Schwarzfahrer	12.5
Schwärzung	5.6
Schweigepflicht	6.2
Screenig-Verfahren	6.1
Sicherheitskonzept	5.1
Sichtblende	9.3
Sitzungsniederschrift	5.2
Sozialhilfe	11.2; 11.6
Stasiüberprüfung	6.3
Sterbebücher	5.13
Stiftung Datenschutz	2.1
Straßenverkehr Tunnel	13.4
Telekommunikationsverkehrsdaten	10.1
Terrorismusbekämpfung	3.2; 3.3, 8.1
Tracking	14.4
Transparenzgebot	12.3
Übermittlungssperren	2.4
Umsatzsteuernachschau	9.2
Umweltinformationsgesetz	12.1
Verdachtsgewinnung	7.4
Verhaltens- und Leistungskontrol-	6.1

le	
Verkehrszählung	12.7
Versorgungsunternehmen	12.3
Videüberwachung	2.3; 5.5; 6.1; 6.4; 12.5; 12.7; 13.4; 13.5
VISkompakt	15.1
Volltextrecherche	8.2
Vorratsdatenspeicherung	3.2; 10.1
Webanalyseprogramm	4.1
WebBug	14.4
Whistleblowing	6.1
Wohngeldantrag	5.6
Zeiterfassung	5.7
Zensus 2011	2.4
zentrales Personenstandsregister	5.12
Zeugnis	11.8
Zugriffsrecht	9.1
Zulassungsstelle	12.6
Zuverlässigkeitsprüfung	7.2; 7.3