TLfDI

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

2022

5. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

5. Tätigkeitsbericht zum Datenschutz nach der DS-GVO | 2022

TLfDI

Vorbemerkungen zum Sprachgebrauch

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

Impressum

Herausgeber:	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI) Postfach 90 04 55, 99107 Erfurt Telefon: +49 (361) 57-3112900 E-Mail: poststelle@datenschutz.thueringen.de Internet: https://www.tlfdi.de
Druck:	THÜRINGER LANDESAMT FÜR BODENMANAGEMENT UND GEOINFORMATION (TLBG)
Layout Umschlag:	Druckerei Wittnebert, Erfurt Inh. Ulrich Janzen e. K. Internet: www.wittnebert.de
Endverarbeitung:	TLBG
Bildernachweis:	TLfDI. Siehe bitte auch Bilduntertitel im Text.
Redaktionsschluss:	Juni 2023

5. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2022
Zitiervorschlag: 5. TB DS-GVO LfDI Thüringen

Der 5. Tätigkeitsbericht DS-GVO steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Juni 2023

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser,

es fällt beim Blick in den Tätigkeitsbericht des Jahres 2022 auf: Die Corona-Pandemie ist nicht mehr das alles beherrschende Thema, auch wenn es noch einige Fälle in diesem Zusammenhang gegeben hat. Andere Datenschutzthemen haben wieder mehr an Bedeutung gewonnen. Der Bericht greift zunächst wichtige Themengebiete in allgemeiner Form auf. Besondere Bedeutung hatte dabei für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage, ob Microsoft 365 datenschutzkonform betrieben werden kann.
Es wird dann im Bericht, getrennt nach öffentlichem und nicht-öffentlichem Bereich, über exemplarische Fälle berichtet, die einen Querschnitt durch die Tätigkeit des TLfDI im Berichtsjahr darstellen. Am Ende finden sich die Entschließungen und sonstigen Entscheidungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, deren Mitglied auch der TLfDI ist, sowie Informationen zu Veranstaltungen des TLfDI im Rahmen seiner Öffentlichkeitsarbeit.
Die Leistung einer Behörde steht und fällt mit ihren Mitarbeiterinnen und Mitarbeitern. Sie haben auch in diesem Jahr mit großem Einsatz die gleichbleibend hohe Zahl an Posteingängen bewältigt, wofür ich ihnen ausdrücklich meinen Dank aussprechen möchte. Dies war nur möglich, indem befristet zusätzlich Beschäftigte eingestellt wurden. Es ist mir ein sehr wichtiges Anliegen, diesen Personen, die für die Tätigkeit der Behörde dringend gebraucht werden, eine Festanstellung bieten zu können. Leider bot die Haushaltsgesetzgebung diese Möglichkeit nicht. Mangels entsprechender Stellen konnten leider auch keinen neuen Mitarbeiter:innen eingestellt werden – befristete Arbeitsverhältnisse sind angesichts des Fachkräftemangels nicht mehr zeitgemäß und der TLfDI muss darauf achten, dass die ihm von der Datenschutzgrundverordnung eingeräumte angemessene Personalausstattung auch Realität wird.

Ich wünsche Ihnen bei der kurzweiligen Lektüre meines 5. Tätigkeitsberichts zum Datenschutz nach der DS-GVO nützliche Erkenntnisse.

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

1. Themengebiete

© Cevahir - Datenaustausch - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik

Die Corona-Pandemie war im Berichtszeitraum nicht mehr das alles beherrschende Thema. Es gewannen nun auch andere datenschutzrechtliche Fragen wieder mehr Raum.

Auch beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war die Corona-Pandemie im Jahr 2022 nicht mehr das alles beherrschende Thema. Zwar gibt es immer noch einige Beschwerden oder Fragen zu Datenverarbeitungen in diesem Zusammenhang. Es ist aber festzustellen, dass nun auch andere datenschutzrechtliche Fragen wieder an Bedeutung gewinnen.
Ein wichtiges Thema war die Frage, ob Microsoft 365 datenschutzrechtskonform betrieben werden kann. In Thüringen ist diese Frage vor allem für den Schulbereich von Bedeutung (vergleiche Nummer 1.5).
Daneben gab es einen bunten Strauß an unterschiedlichen Problemfeldern, von denen dieser Bericht einige exemplarisch aufgreift. Der Be-

richt stellt eine repräsentative Auswahl aus den Fällen und Themengebieten dar, mit denen sich der TLfDI im Berichtsjahr befasst hat, von der Videoüberwachung in der Arztpraxis (vergleiche Nummer 3.4) über den Einsatz von Zoom (vergleiche Nummer 1.6) bis hin zur vermuteten Scheinehe (vergleiche Nummer 2.3).

Einige statistische Angaben:

Im Jahr 2022 gab es 20.592 Posteingänge beim TLfDI. Die Zahl ist damit auf einem annähernd gleich hohen Niveau geblieben.

Es wurden im Berichtsjahr 112 Bußgeldverfahren eröffnet. Davon endeten bereits neun mit einem Bußgeldbescheid. Insgesamt wurden beim TLfDI 55 Bußgeldbescheide im Jahr 2022 erlassen, etwas weniger als im Vorjahr, wovon 42 bis zum Ende des Berichtszeitraumes Rechtskraft erlangten. Die Höhe der insgesamt festgesetzten Bußgelder betrug 31.165 Euro. Der TLfDI erließ acht Bußgeldbescheide nach Art. 83 Abs. 4 Datenschutz-Grundverordnung (DS-GVO). Diese betreffen alle unterlassenen Meldungen nach Art. 33 DS-GVO (Datenpannen) und richteten sich gegen Unternehmen. Weiterhin wurden 46 Bußgeldbescheide nach Art. 83 Abs. 5 DS-GVO erlassen. Der überwiegende Teil der Bußgeldbescheide richtete sich gegen die Betreiber von unbefugter Videoüberwachung – sowohl im Privatbereich als auch gegen Unternehmen. Bei den Verstößen im Polizeibereich ist eine positive Entwicklung festzustellen. Im Berichtsjahr 2022 wurden insgesamt fünf Bußgeldbescheide wegen unbefugten Abrufen in polizeilichen IT-Systemen durch Beamte der Thüringer Polizei erlassen. Im Vorjahr (2021) lag die Anzahl der Bußgeldbescheide im Polizeibereich mit 24 deutlich höher.

Ferner erließ der TLfDI einen Bußgeldbescheid nach § 43 Abs. 2 Nr. 2 Bundesdatenschutzgesetz alter Fassung. Hierbei wurden unter anderem datenschutzrechtliche Verletzungen bei der Einführung einer elektronischen Legitimation der Schüler bei der Mittagsversorgung an einer Gesamtschule sanktioniert.

Insgesamt ist die Zahl der Meldungen der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO mit 261 im Vergleich zum Vorjahr leicht zurückgegangen. Darunter waren etliche Fälle, in denen Patientendaten oder Bewerberdaten an einen falschen Adressaten versandt worden waren oder es aus anderen Gründen zu einer Offenbarung von personenbezogenen Daten gekommen war, ohne dass hierzu eine Berechtigung bestanden hätte. Eine Vielzahl betraf Cyberangriffe auf die IT-Infrastruktur der Verantwortlichen.

1.2 Vorratsdatenspeicherung möglich – aber nicht von allen und ohne Anlass!

Die Vorratsdatenspeicherung ist in Deutschland seit Jahren umstritten. So umstritten, dass das entsprechende Gesetz seit fünf Jahren unangewendet in der Schublade liegt. In diesem Jahr entschied dann der Europäische Gerichtshof – und erteilte den staatlichen Kontrollwünschen zum großen Teil eine Absage.

In den letzten Jahren hat sich der Europäische Gerichtshof in mehreren Urteilen zur Vorratsdatenspeicherung geäußert. Denn verschiedene Mitgliedstaaten hatten ähnliche Regelungen wie in Deutschland erlassen, die eine anlassbezogene Speicherung von Verbindungsdaten (Meta-Daten) nahezu aller Bürgerinnen und Bürger vorsahen. Doch das Europarecht schützt die Vertraulichkeit auch und gerade der Online-Kommunikation und die Privatsphäre. Die europarechtliche Zulässigkeit war deshalb seit langem fraglich. Grund genug, über das Urteil des Europäischen Gerichtshofs zur deutschen Vorratsdatenspeicherung zu berichten – auch wenn es nicht unmittelbar die DS-GVO betrifft.

Zum Hintergrund: Die Vorratsdatenspeicherung funktioniert so, dass in einem ersten Schritt die privaten Internet-Infrastrukturanbieter verpflichtet werden, die Verbindungsdaten ihrer Kunden zu speichern. Das betrifft bei Telefonaten beispielsweise die beteiligten Telefonnummern, die Uhrzeit und die genutzte Funkzelle. Bei der Internetnutzung werden die IP-Adressen der Endgeräte und der angerufenen Server gespeichert, also im Ergebnis eine Liste der aufgerufenen Webseiten. Die Speicherung erfolgt dann je nach Datenkategorie vier oder zehn Wochen lang. In einem zweiten Schritt müssen die Anbieter den Strafverfolgungsbehörden Zugang zu den so gespeicherten Daten gewähren. Dafür benötigen diese dann unter anderem einen richterlichen Beschluss.

Sie wenden sich gegen die ihnen durch § 113a Abs. 1 in Verbindung mit § 113b Telekommunikationsgesetz (TKG) auferlegte Speicherpflicht. Die im Jahr 2015 mit dem Gesetz zur Mindestspeicherpflicht und Höchstspeicherdauer von Verkehrsdaten eingeführte Regelung sah eigentlich vor, dass die Vorratsdatenspeicherung ab 1. Juli 2017 beginnen sollte.

Gegen das deutsche Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, durch das die

§§ 113a, 113b des Telekommunikationsgesetzes durch die neuen §§ 113a bis 113g ersetzt wurden, hatten zwei private Internetinfrastrukturanbieter geklagt. Im Laufe des Rechtsstreits wurden die entscheidenden europarechtlichen Fragen dem Europäischen Gerichtshof vorgelegt, der entschied, dass die deutsche Regelung zur Vorratsdatenspeicherung nicht mit dem Europarecht vereinbar ist. Konkret ging es um die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58, der Freiheit und Sicherheit in einen Kompromiss bringen soll. Damit können auch Verkehrsdaten von Thüringer Bürgern nicht mehr nach diesen Bestimmungen gespeichert werden.

Maßgeblich für die Entscheidung war, dass die nach dem deutschen Gesetz anlasslos und flächendeckend zu speichernden Daten es erlauben würden, ein umfangreiches und detailliertes Profil jeden Bürgers zu erstellen. Deshalb stellt bereits die Speicherung dieser Daten (die erste Stufe) einen schwerwiegenden Eingriff in die Grundrechte dar. Darauf, wie hoch die Hürden für den späteren Datenzugriff der Behörden sind (zweite Stufe), kommt es gar nicht zentral an. Doch auch die staatlichen Interessen an der Bekämpfung und Verfolgung von schweren Straftaten oder Bedrohungen der nationalen Sicherheit sind zu berücksichtigen.

Der Gerichtshof fand einen Kompromiss: Eine umfassende und anlasslose Speicherung, wie im deutschen Gesetz vorgesehen, ist für ihn unzulässig. Denn dann bliebe von den Grundrechten auf Achtung des Privat- und Familienlebens sowie auf den Schutz personenbezogener Daten nicht mehr viel übrig – die Ausnahme von Privatsphäre und Vertraulichkeit würde zur Regel. Geschieht die Überwachung jedoch nicht flächendeckend oder bestehen ganz besondere Umstände, kann eine Vorratsdatenspeicherung rechtmäßig sein. In diesen Fällen geht die Abwägung zugunsten der staatlichen Sicherheitsinteressen aus.

Der Gerichtshof benennt in seinem Urteil beispielhaft einige solcher Situationen. Zunächst rechtfertigt eine reale und aktuelle oder zumindest vorhersehbare ernste Bedrohung der nationalen Sicherheit eine Vorratsdatenspeicherung, wenn sie gerichtlich überprüfbar ist und nur für eine begrenzte Zeit geschieht. Daneben genügt auch das Ziel der Bekämpfung schwerer Kriminalität, wenn nicht (nahezu) alle Bürger überwacht werden. Die Eingrenzung kann dabei entweder anhand objektiver Kriterien geschehen, die einen Kreis von Personen bestimmen, von denen eine größere Gefahr ausgeht als von anderen Bürgern. Bei diesem Personenkreis ist eine anlasslose Vorratsdatenspeicherung dann zulässig. Ebenfalls möglich ist die geografische Eingrenzung:

Orte, die von vielen Menschen besucht werden, die strategisch wichtig sind (Bahnhöfe, Flughäfen und so weiter) oder solche, an denen Kriminalität statistisch häufiger stattfindet, dürfen anlasslos überwacht werden.
Kurz gesagt, macht der Europäische Gerichtshof folgende Vorgabe: entweder flächendeckend, aber nicht anlasslos, oder anlasslos, aber nicht flächendeckend. Damit hat der Europäische Gerichtshof die Privatsphäre der Bürger gegen den Druck vieler Mitgliedstaaten verteidigt – Grundrecht ist schließlich Grundrecht. Und daran ändert sich auch nichts, nur weil es schwierig sein mag, die zulässigen Ausnahmefälle präzise zu bestimmen. Doch ein für alle Mal geklärt ist der Streit mit dem Urteil sicherlich nicht. Die Verlockung, die technischen Möglichkeiten zur nahezu unbegrenzten Überwachung auch tatsächlich zu nutzen, dürfte früher oder später zu erneuten Vorstößen führen. Es bleibt zu hoffen, dass der Europäische Gerichtshof dem auch in Zukunft Grenzen setzen wird.

1.3 Leitlinien des EDSA

Viele Artikel der Datenschutz-Grundverordnung lassen einen großen Interpretationsspielraum zu. Der Europäische Datenschutzausschuss, kurz EDSA (auf Englisch: European Data Protection Board, kurz EDPB), veröffentlicht daher Leitlinien zur Präzisierung der Datenschutz-Grundverordnung und zur Förderung einer harmonisierten Auslegung des europäischen Datenschutzrechts.

Im Europäischen Datenschutzausschuss (EDSA) sind die Leiter der nationalen Datenschutzaufsichtsbehörden aller Mitgliedsstaaten der Europäischen Union sowie der Europäischen Datenschutzbeauftragte vertreten. Der Ausschuss verfügt als Einrichtung der Europäischen Union über eine eigene Rechtspersönlichkeit. Da Deutschland aufgrund seiner föderalen Struktur mehrere Datenschutzaufsichtsbehörden hat, wird von diesen ein gemeinsamer Vertreter ernannt, der die deutschen Datenschutzaufsichtsbehörden in dem Ausschuss vertritt. Derzeit nimmt diese Position der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wahr, er wird vertreten vom Bayerischen Landesbeauftragten für den Datenschutz. Der EDSA handelt bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse unabhängig und weisungsfrei gemäß Art. 69 DS-GVO.

Die Aufgaben des EDSA sind in Art. 70 DS-GVO normiert. Dazu zählt unter anderem auch die Bereitstellung von Leitlinien, um die einheitliche Anwendung der DS-GVO sicherzustellen. Der EDSA verfügt über Unterarbeitsgruppen, die sogenannten Expert Subgroups (= Experten-Unterarbeitsgruppen), die diese Leitlinien für den Ausschuss vorbereiten.
Die Leitlinien des EDSA spielen auch für die Prüfpraxis des Thüringer Landesbeauftragten für den Datenschutz (TLfDI) eine große Rolle, geben Sie doch für die vielen unbestimmten Rechtsbegriffe der DS-GVO eine Auslegungshilfe, die eine ähnliche Wirkung wie Verwaltungsvorschriften entfaltet.
Beispielhaft soll an dieser Stelle auf die entsprechende Leitlinie zum Auskunftsrecht der betroffenen Person gemäß Art. 15 DS-GVO hingewiesen werden, die sich zwar noch in der öffentlichen Konsultation, also abschließenden Beratung, befindet, aber schon in dieser Version auf der Internetseite des EDSA veröffentlich wurde. Das Recht auf Auskunft ist eines der zentralen Betroffenenrechte der DS-GVO und es wird häufig davon Gebrauch gemacht. Daher ist es sinnvoll und wichtig, dass hierfür Leitlinien herausgegeben werden, die für mehr Klarheit und eine einheitlichere Anwendung der Regelungen sorgen. So legen die Leitlinien unter anderem fest, welche Daten vom Recht auf Auskunft umfasst sind, welche Maßnahmen des Verantwortlichen für die Identifizierung getroffen werden müssen oder wann es sich um einen exzessiven Antrag handelt.
Nachzulesen sind die Leitlinien auf der Internetseite des EDSA unter https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de.
Diese liegen jedoch bislang nur in englischer Sprache vor.

1.4 Die kommunalen Datenschutzbeauftragten – unverzichtbar

Die behördlichen Datenschutzbeauftragten sind in den Thüringer Kommunen unverzichtbar und daher auch vom Gesetzgeber als verpflichtendes Instrument vorgesehen. Ihre Arbeit ist für die datenschutzgerechte Ausgestaltung kommunaler Prozesse und Tätigkeiten nicht wegzudenken.

Die Kommunen in Thüringen erbringen sehr viele Verwaltungsleistungen für die Bürgerinnen und Bürger. Damit einher geht auch die Verarbeitung einer Vielzahl unterschiedlichster personenbezogener

Daten. Um diese Aufgaben datenschutzgerecht zu meistern, bedarf es der Hilfe der behördlichen Datenschutzbeauftragten.
Die Datenschutz-Grundverordnung (DS-GVO) und auch das Thüringer Datenschutzgesetz (ThürDSG) drücken sich dabei in Art. 37 Abs. 1 DS-GVO und § 13 Abs. 1 ThürDSG klar aus; öffentliche Stellen müssen einen Datenschutzbeauftragten bestellen. Dieser Verpflichtung sind nach Kenntnis des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bislang die Kommunen grundsätzlich nachgekommen. An der einen oder anderen Stelle hakte es zwar, aber auch hier konnten die Probleme mit Hilfe des TLfDI gelöst werden. So wurde eine Verwaltungsgemeinschaft (VG) seitens des TLfDI darauf aufmerksam gemacht, dass ein behördlicher Datenschutzbeauftragter sowohl für die VG als auch für die dazugehörigen Gemeinden bestellt werden muss. Dies holten die Gemeinden, die bis dato noch keinen eigenen behördlichen Datenschutzbeauftragten bestellt hatten, dann unverzüglich nach. An dieser Stelle weist der TLfDI darauf hin, dass gemäß § 13 Abs. 3 ThürDSG auch von der Möglichkeit Gebrauch gemacht werden kann, für mehrere öffentliche Stellen einen gemeinsamen Datenschutzbeauftragten zu bestellen. Im Sommer 2022 bat der TLfDI alle beim TLfDI gemäß Art. 37 DS-GVO gemeldeten Datenschutzbeauftragten zu prüfen, ob deren Daten noch korrekt sind. Hintergrund hierfür ist, das Meldeportal, das die Datenschutzbeauftragten nutzen, um ihre Bestellung anzeigen, möglichst aktuell zu halten. Dieser Bitte kamen die Datenschutzbeauftragten nach.
Zu den Aufgaben eines behördlichen Datenschutzbeauftragten gehören unter anderem die Überwachung der Einhaltung der Datenschutz-Grundverordnung (DS-GVO), des Thüringer Datenschutzgesetzes und anderer datenschutzrechtlicher Bestimmungen (siehe § 15 Abs. 1 ThürDSG sowie der auf Grundlage der JI-Richtlinie erlassenen Rechtsvorschriften (siehe § 15 Abs. 3 ThürDSG), die Unterrichtung und die Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen personenbezogener Daten durchführen, Schulungen zum Datenschutz, die Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese zu sein. Zudem ist den behördlichen Datenschutzbeauftragten vor der erstmaligen Inbetriebnahme einer Verarbeitungstätigkeit das dafür erforderliche Verzeichnis mit der Gelegenheit zur Stellungnahme vorzulegen. Schließlich sind die behördlichen Datenschutzbeauftragten bei einer Datenschutz-Folgenabschätzung einzubeziehen. Man kann unschwer erkennen, dass die Aufgaben sehr

vielfältig sind und sie daher eines umsichtigen und fachlich befähigten Datenschutzbeauftragten bedürfen, dessen Arbeit sich auch in einer angemessenen Vergütung widerspiegeln sollte.
§ 14 Abs. 7 ThürDSG sieht vor, dass die/der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen kann. Die öffentliche Stelle hat aber sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen und dem behördlichen Datenschutzbeauftragten für die Erfüllung seiner Aufgaben weiterhin hinreichende Arbeitszeit verbleibt. In vielen Kommunen können die behördlichen Datenschutzbeauftragten ihr Amt nur im Nebenamt wahrnehmen. Doch gerade dort, wo viele Aufgaben, die eine öffentliche Stelle zu bewältigen hat, zusammenkommen, wäre es wünschenswert, wenn die/der behördliche Datenschutzbeauftragte nur ihre/seine Aufgaben als Datenschutzbeauftragte(r) wahrnehmen könnte und von Fachaufgaben befreit wäre.
Einige Städte haben einen hauptamtlich bestellten behördlichen Datenschutzbeauftragten, dessen alleinige Aufgabe es ist, die öffentliche Stelle bei der Sicherstellung des Datenschutzes zu unterstützen. Zu verkennen ist natürlich nicht, dass sich größere Städte einen hauptamtlichen Datenschutzbeauftragten eher leisten können als eine kleine Gemeinde.
Um einen regelmäßigen Austausch der kommunalen Datenschutzbeauftragten zu gewährleisten, gibt es bereits seit vielen Jahren den Arbeitskreis der kommunalen Datenschutzbeauftragten. Auch der TLfDI nimmt an dessen Sitzungen teil. In einem konstruktiven Austausch können dabei Datenschutzprobleme, die möglicherweise alle Kommunen in Thüringen betreffen, angesprochen und Lösungswege erörtert werden.

1.5 Microsoft 365 in der Schule

Eine datenschutzkonforme Nutzung von Microsoft 365 kann von Verantwortlichen auf der Grundlage der von Microsoft bereitgestellten Unterlagen derzeit nicht nachgewiesen werden. Ein Einsatz dieses Clouddienstes in der Schule wäre nur zulässig, wenn die verantwortliche Schulleitung ihrer Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO nachkommen könnte, was sich indes nicht abzeichnet.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wies bereits in seinem 4. Tätigkeitsbericht für

das Jahr 2021 unter Nummer 1.7 darauf hin, dass die Nutzung von Microsoft 365 in Schulen aus datenschutzrechtlicher Sicht als sehr kritisch zu sehen ist. Aus diesem Grund wurde der Umgang mit Microsoft 365 in der Schule wie im Jahr zuvor weiterhin in der vom TLfDI und der Kultusministerkonferenz (KMK) gegründeten Arbeitsgruppe (AG) Datenschutz auf die Tagesordnung gesetzt. Als Unterstützungsleistung für ein geplantes Gespräch der KMK mit Vertretern von Microsoft erarbeitete der TLfDI gemeinsam mit den Mitgliedern seiner beiden Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz einen Fragenkatalog zu datenschutzrechtlichen Unklarheiten und fehlenden Erläuterungen in den von Microsoft veröffentlichten Unterlagen zu Microsoft 365. Im Oktober 2022 erfolgte dann das Gespräch mit Vertretern von Microsoft bei der KMK in Berlin. Der TLfDI war über den Auftritt von Microsoft enttäuscht und brachte die Gefahr zum Ausdruck, dass Microsoft wie bereits in der Vergangenheit auf Zeit spiele und man diese Zeit nicht vertun solle. Ziel sei es, schnell zu Ergebnissen zu kommen. Das Gespräch brachte leider nach Einschätzung des TLfDI keine greifbaren Lösungen und Microsoft ging auf die vorgetragenen Probleme nicht wirklich ein.

Bereits zuvor hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Arbeitsgruppe Microsoft Onlinedienste eingesetzt, die sich seit Ende 2020 mit der Microsoft 365-Problematik beschäftigt hatte. Neben der Prüfung der datenschutzrechtlich relevanten Unterlagen erfolgten in dieser Zeit 14 Videokonferenzen mit Microsoft. Unter Berücksichtigung dieser Gespräche und des von Microsoft bereitgestellten Datenschutznachtrags vom 15. September 2022‘ erstellte die Arbeitsgruppe Microsoft Onlinedienste einen Bericht zur datenschutzrechtlichen Beurteilung von Microsoft 365. Auf Grundlage dieses Berichts (Kurzfassung: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf) veröffentlichte die DSK am 24. November 2022 die Festlegung (https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf) mit dem Inhalt, dass „der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‘Datenschutznachtrags vom 15. September 2022’ nicht geführt werden kann.“

Die Bewertung der Datenschutzkonferenz wendet sich nicht direkt an Microsoft, sondern an die Verantwortlichen und damit auch an die Schulleitungen und besagt, dass Microsoft 365 für schulische Zwecke derzeit nicht datenschutzrechtskonform genutzt werden kann. Die Schulen (und andere Verantwortliche) müssten nach Art. 5 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) nachweisen können, dass Microsoft 365 transparent und rechtmäßig verwendet werden kann. Die Führung eines solchen Nachweises ist aber nicht möglich, solange Microsoft seinen eigenen Unterlagen zufolge personenbezogene Daten für eigene Zwecke verwendet und auch keine weiteren Angaben macht, welche personenbezogenen Daten von wem zu welchem Zweck verarbeitet werden. Selbst das Verwenden des Clouddienstes auf der Grundlage einer Einwilligung der Erziehungsberechtigten, der volljährigen Schülerinnen und Schüler oder Lehrkräfte ist unzulässig, da der Schulleitung weder bekannt ist, ob mit Microsoft 365 personenbezogene Daten von Kindern oder Lehrkräften von Microsoft zu eigenen Zwecken verarbeitet werden, und falls dies der Fall ist, für welche Zwecke dies erfolgt. Im Ergebnis kann die Schulleitung entgegen der Bestimmung von Art. 4 Nr. 11 DS-GVO die Eltern und die Lehrkräfte gar nicht in informierter Weise einwilligen lassen und kann auch nicht ihren Informationspflichten nach Art. 13 DS-GVO nachkommen. Derart erteilte Einwilligungen wären unwirksam (!) und damit fehlte es der verantwortlichen Schulleitung an einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DS-GVO, die Daten mit Microsoft 365 verarbeiten zu dürfen.

Überdies kann vor diesem Hintergrund die Schulleitung als Verantwortlicher Microsoft als Auftragsverarbeiter gar nicht anweisen, die Daten in bestimmter Weise zu verarbeiten oder eben nicht zu verarbeiten, solange sich Microsoft vorbehält, die Daten für eigene Zwecke zu verarbeiten. Hierin liegt ein weiterer Verstoß, nämlich gegen Art. 28 DS-GVO. Hinzu kommt – wie bei nahezu allen US-amerikanischen Unternehmen – die Problematik von möglichen Zugriffen auf personenbezogene Daten von Nicht-Amerikanern durch US-amerikanische Sicherheitsbehörden, wogegen kein Rechtsschutz besteht. Diese und weitere Probleme greift der Europäische Gerichtshof in seinem Urteil vom 16. Juli 2020, C-311/18 „Schrems II“ auf. Der TLfDI wird, wie die anderen Datenschutzaufsichtsbehörden auch, mit den Verantwortlichen im öffentlichen und nicht-öffentlichen Bereich den Kontakt suchen, um eine verhältnismäßige Umsetzung dieser Rechtslage zu erörtern. Hierbei werden zeitliche Aspekte und alternative

Pfade Gegenstand der Erörterung sein. Der TLfDI hat übrigens den Thüringer Schulleitungen bereits vor zwei Jahren mitgeteilt, dass Microsoft 365 (vormals Microsoft Office 365) nicht empfohlen werden kann. Inzwischen ist klar, dass die Nutzung dieses Clouddienstes sogar datenschutzrechtlich unzulässig ist.
Das **Thüringer Ministerium** für Bildung, Jugend und Sport (TMBJS) hat „Antworten auf häufig gestellte Fragen zum Datenschutz in Schulen“ auf seiner Webseite veröffentlicht. Darin weist das TMBJS unter Ziffer 7.5 darauf hin, dass Cloud-Angebote nichteuropäischer Anbieter, zum Beispiel **Microsoft-Office 365, in Thüringer Schulen nicht genutzt werden dürfen**. Die in Zusammenarbeit mit dem TLfDI entwickelten FAQs sind zu finden unter https://bildung.thueringen.de/fileadmin/schule/medien/datenschutz-in-schulen/FAQ_Datenschutz_in_Schulen_2022-10-19.pdf.

1.6 Einsatz von Zoom an einer Thüringer Hochschule

Der Einsatz von Zoom kann nur unter bestimmten Bedingungen in Vorlesungen stattfinden. Für Videokonferenzen, in denen sensiblere Daten verarbeitet werden, etwa bei der Durchführung von Onlineprüfungen oder uniinternen Sitzungen, muss aber auf andere, datenschutzgerechte Videokonferenzsysteme, die weitere Sicherheitsmaßnahmen erfüllen, zurückgegriffen werden.

Seit dem Beginn der Corona-Pandemie im Jahre 2020 werden in den Bildungseinrichtungen vermehrt Videokonferenzen als Kommunikationsmöglichkeit eingesetzt, insbesondere zur Aufrechterhaltung eines Distanzlehrbetriebs. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) musste sich in diesem Zusammenhang aufgrund von Anfragen von besorgten Eltern von Schulkindern und Studierenden mit vielen auf dem Markt angebotenen Videokonferenzsystemen beschäftigen, deren Anbieter oftmals ihren Unternehmenssitz außerhalb der Europäischen Union haben.
Durch Beschwerden von Studierenden wurde der TLfDI darauf aufmerksam, dass eine Thüringer Universität seit dem Sommersemester 2020 das Videokonferenzsystem Zoom nutzt: der Betreiber ist ein US-amerikanisches Softwarewareunternehmen. Die Universität führt mit diesem Dienst Online-Lehrveranstaltungen sowie mündliche und

schriftliche Online-Prüfungen durch und nutzt Zoom auch für inneruniversitäre Lehr- und Konferenzveranstaltungen des Universitätspersonals.
Die Universitätsleitung vertritt die Meinung, dass der Einsatz des Videokonferenzsystems zulässig sei, weil es zur Aufgabenerfüllung der Universität, etwa der Aufrechterhaltung des Lehrbetriebs erforderlich, sei. Es gebe kein von der Universität selbst betriebenes System, welches bei teilweise hunderten Teilnehmern annehmbar verbindungsstabil sei. Nach Prüfung der Stellungnahme der Universität kam der TLfDI aber zu dem Ergebnis, dass Zoom bei den Videokonferenzen anfallende personenbezogene Daten nicht nur ausschließlich für Zwecke der Universität in Forschung und Lehre, sondern auch zu anderen, gegebenenfalls eigenen Zwecken verarbeitet. Deswegen können nicht alle Bedingungen, die nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO) an einen Auftragsverarbeitungsvertrag zu stellen sind, erfüllt werden. Als Auftragsverarbeiter darf Zoom ausschließlich für Zwecke der Universität und keinesfalls für eigene Zwecke, zum Beispiel Marketingzwecke oder Profilbildung, Daten der Nutzer verarbeiten. Darüber hinaus kann Zoom als Produkt eines Unternehmens mit Sitz in den USA entsprechend der vom Europäischen Gerichtshof in dessen Urteil vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II“) festgestellten Ungültigkeit des sogenannten Privacy Shields – einer Absprache zwischen der Europäischen Union (EU) und den USA, wonach die Grundsätze des Datenschutzes in der EU von US-amerikanischen Unternehmen einzuhalten sind – kein angemessenes Schutzniveau für eine Verarbeitung personenbezogener Daten in den USA garantieren. Darüber hinaus können auch von US-amerikanischen Firmen in der EU verarbeitete Daten von US-Sicherheitsbehörden eingesehen werden, ohne dass hiergegen (derzeit) ein ausreichender Rechtsschutz für die hiervon betroffenen Personen besteht.
Zusätzlich musste der TLfDI feststellen, dass bei jedem Beitritt zu einer Zoom-Konferenz, etwa für eine Online-Vorlesung, der Server zoom.us kontaktiert wird. Nach den Aussagen von Zoom geschieht dies, um für die Konferenzraum-Nummer den zuständigen lokalen Server zu ermitteln, über welchen dann die eigentliche Konferenz stattfindet. Die Kontaktaufnahme ist also eine Art „Vermittlungsanfrage“. Da keine spezielle Rechtsgrundlage die Teilnahme an Zoom regelt, müssen die Studierenden zuvor bei der Universität in die Verarbeitung ihrer Daten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) in Ver-

bindung mit Art. 7 DS-GVO einwilligen. Die Studierenden haben danach das Recht, ihre Einwilligung jederzeit zu widerrufen. Ein solcher Widerruf macht aber die weitere Speicherung der erhobenen Daten unzulässig. Sie müssten gelöscht werden. Eine derartige Löschung kann aber durch die Universität entgegen den Bestimmungen der DS-GVO (Art. 17 Abs. 1 Buchstabe b) DS-GVO) nicht durchgeführt werden, da es sich teilweise um Prüfungsleistungen handelt. Das Erfordernis des Widerrufs kann von der Universität daher gar nicht erfüllt werden.
Zusätzlich ist auch fraglich, ob überhaupt von einer Freiwilligkeit der Nutzung von Zoom bei den Studierenden auszugehen ist oder ob den Studierenden bei einer Nicht-Einwilligung Nachteile entstehen, weil die entsprechenden Vorlesungen dann nicht besucht werden können. Im Ergebnis wurde die Universität wegen der Nutzung von Zoom vor Erlass einer Maßnahme nach Art. 58 Abs. 2 DS-GVO förmlich angehört.
Zwischenzeitlich musste aufgrund des Inkrafttretens des neuen Telekommunikationsgesetzes und des Telekommunikation-Telemedien-Datenschutz-Gesetzes entschieden werden, ob der TLfDI (und auch die anderen Landesdatenschutzbeauftragten) weiterhin die Zuständigkeit für die Aufsicht über Verantwortliche besitzt, die solche Videokonferenzsysteme einsetzen, oder ob diese Aufgabe zukünftig vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wahrzunehmen ist. Damit eng verknüpft ist die Frage, ob die Hochschulen, aber auch die Schulen, unter der neuen Gesetzeslage als Nutzer des Videokonferenztools verantwortlich im Sinne des Datenschutzes sind oder ob die Verantwortlichkeit ausschließlich beim Anbieter liegt, vorliegend also Zoom. Das Ergebnis in der Datenschutzkonferenz war dann eindeutig: Nach einstimmiger Feststellung bleiben die Datenschutzaufsichtsbehörden für Schulen und Hochschulen bei der Nutzung von Videokonferenzdiensten weiterhin zuständig. Siehe zu TOP 6: https://www.datenschutzkonferenz-online.de/media/pr/20221129_Protokoll_3_Zwischenkonferenz.pdf.
Um die Problematik einer abschließenden Klärung zuzuführen, hat sich der TLfDI entschlossen, der Nutzung von Zoom ausnahmsweise dann zuzustimmen, wenn die Universität die Kriterien der sogenannten Hessischen Lösung erfüllt. Danach muss zwischen der Universität und dem Anbieter Zoom ein weiterer Auftragsverarbeiter mit Sitz und Standort der Datenverarbeitung im Wirkungsbereich der DS-GVO zwischengeschaltet werden. Dieser stellt einen Server zur Verfügung,

auf dem die Inhaltsdaten der Kommunikation gehostet werden, die zusätzlich Ende-zu-Ende verschlüsselt sind. Auf diese Daten kann dann weder von Zoom noch von US-amerikanischen Sicherheitsbehörden zugegriffen werden. Nach wie vor für Zoom zugänglich bleiben dann noch die Nutzerdaten (Studierende, Lehrende) sowie anfallende Metadaten. Aus diesem Grund muss die Hochschule die Accounts der Nutzer mit einem von der Hochschule lokal betriebenen Identitätsmanagementsystem pseudonymisieren und alle Studierenden auf die Verwendung des zur Verfügung stehenden Virtual Private Networks (VPN) – eine Netzwerkverbindung, die von unbefugten Dritten nicht eingesehen werden kann – hinweisen. Darüber hinaus sind weitere technische und organisatorische Maßnahmen von der Universität zu ergreifen, zum Beispiel die Abschaltung der Cloud-Aufzeichnungsfunktion.
Die Nutzung von Zoom muss sich auf Lehrveranstaltungen beschränken. Für andere Zwecke der Hochschule, die einem höheren Schutzbedarf unterliegen, etwa die Durchführung von Online-Prüfungen, darf Zoom auch in der beschriebenen Konstellation nicht genutzt werden. Die Universität muss für solche Fälle den Studierenden und den Lehrpersonen ein datenschutzgerechtes Alternativprodukt bereitstellen – oder eben Prüfungen wie bisher präsent durchführen.
Die Universitätsleitung hat mitgeteilt, die Kriterien des „Hessischen Modells“ vollumfänglich zu erfüllen und aktuell auf das Produkt Zoom X umzustellen. Hierbei übernimmt die Telekom Deutschland GmbH die Aufgabe des oben genannten Auftragsverarbeiters. Der TLfDI hat die Universität gebeten, ihm eine Registriermöglichkeit einschließlich einer pseudonymisierten E-Mail-Adresse zur Durchführung einer Testkonferenz in Zoom X zur Verfügung zu stellen. Damit wird der TLfDI nachverfolgen, welche Daten wohin übermittelt werden. Dies wird aber erst im Jahre 2023 erfolgen.

1.7 Auskunftsanspruch und Identität des Auskunftssuchenden

Hat der Verantwortliche im Rahmen eines Auskunftsersuchens nach Art. 15 DS-GVO begründete Zweifel an der Identität des Antragstellers und kommt der Auskunftssuchende seiner Pflicht zur Vorlage der hierzu erforderlichen Informationen nicht nach, können ihm die Kosten für die Feststellung seiner Identität auferlegt werden. Steht der

Aufwand zur Identitätsfeststellung in keinem angemessenen Verhältnis zum Informationswert der begehrten Auskunft, kann der Antrag auch abgelehnt werden.

Das Auskunftsrecht der betroffenen Person nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) ist nach Maßgabe des Art. 12 Abs. 5 Satz 1 DS-GVO grundsätzlich kostenfrei. In einem beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) anhängigen Verfahren bezweifelte der Verantwortliche die Identität des Antragstellers. Der Auskunftssuchende weigerte sich, ein Identitätsformular auszufüllen oder sonst wie an der Feststellung seiner Identität mitzuwirken, sodass die Frage aufkam, ob der Verantwortliche die Kosten für die Identitätsfeststellung geltend machen kann oder gar von seiner Pflicht zur Auskunft befreit ist.
Nach Art. 12 Abs. 5 Satz 2 DS-GVO kann bei einem offensichtlich unbegründeten Auskunftsersuchen vom Grundsatz der Unentgeltlichkeit abgewichen werden. Offensichtlich unbegründet ist der Antrag, wenn ein unberechtigter Dritter die Rechte der von einer Datenverarbeitung betroffenen Person geltend macht. Hat der Verantwortliche im Rahmen eines Auskunftsersuchens begründete Zweifel an der Identität des Antragstellers, kann er daher gemäß Art. 12 Abs. 6 DS-GVO geeignete Informationen zur Identifizierung anfordern. Dabei obliegt es dem Betroffenen, die zur Wahrung seiner Rechte geforderten Informationen vorzulegen beziehungsweise glaubhaft zu machen. Kommt er seiner Obliegenheit zur Mitwirkung nicht nach und ist deshalb eine kostenintensive Identitätsprüfung erforderlich, etwa im Wege eines „Postident"-Verfahrens, handelt es sich dabei um eine eigene, vom Betroffenen selbst veranlasste Aufwendung. Diese Aufwendung wird vom Grundsatz der Unentgeltlichkeit nach Art. 12 Abs. 5 Satz 1 DS-GVO nicht erfasst und ist daher vom Betroffenen auch selbst zu tragen. Dies setzt allerdings voraus, dass der Verantwortliche den Antragsteller zuvor über die von ihm zu tragende Kostenlast informiert hat.
Zur Entscheidung, welche Mittel zur Identifizierung des Auskunftssuchenden genutzt werden, sollen alle objektiven Faktoren herangezogen werden, zu denen neben dem Zeitaufwand auch die Kosten der Identitätsfeststellung gehören (Erwägungsgrund 23 zur DS-GVO). Bei der Beurteilung, ob der Betroffene objektiv bestimmbar ist, sind die Kosten zwar nicht maßgebend. Die Anforderung identitätsstiften-

der Daten nach Art. 12 Abs. 6 DS-GVO ist aber eine Ermessensentscheidung, bei der es nicht nur um die Erforderlichkeit des Identitätsnachweises, sondern auch um dessen Verhältnismäßigkeit im engeren Sinne geht, sodass der Aufwand, um den Betroffenen bestimmen zu können, noch in einem angemessenen Verhältnis zum Informationswert der Auskunft stehen muss. Andernfalls kann davon ausgegangen werden, dass der Verantwortliche nicht in der Lage ist, die betroffene Person oder genauer den Antragsteller zu identifizieren, sodass er gemäß Art. 11 Abs. 2 DS-GVO den Antrag auf Auskunft ablehnen kann. Diese Möglichkeit wird durch Art. 12 Abs. 2 DS-GVO nochmals klargestellt. Sieht der Verantwortliche aufgrund des unverhältnismäßigen Identifizierungsaufwands keine Möglichkeit dem Auskunftsersuchen zu entsprechen, muss er den Antragsteller gemäß Art. 12 Abs. 4 DS-GVO hierüber ohne Verzögerung, spätestens jedoch innerhalb eines Monats unterrichten. Dabei muss er sein (erfolgloses) Bemühen um eine Identifizierung glaubhaft machen. Der TLfDI kann dies auf eine Beschwerde des Betroffenen hin überprüfen.
Da im zu prüfenden Fall nachvollziehbare Zweifel an der Identität des Antragstellers bestanden und dieser nicht bereit war, an der Feststellung der Identität mitzuwirken, musste die Auskunft nicht erteilt werden. Auf diese Weise wird vermieden, dass personenbezogene Daten im Rahmen der Beantwortung eines solchen Ersuchens an Dritte übermittelt werden.

1.8 Ist der Betriebsrat Verantwortlicher oder nicht?

Eine Gesetzesänderung schafft Klarheit. In § 79a Satz 2 BetrVG wurde klargestellt: Der Arbeitgeber ist der für die Verarbeitung von personenbezogenen Daten Verantwortliche im Sinne des Art 4 Nr. 7 DS-GVO. Natürlich trifft den Betriebsrat aber weiterhin die Pflicht zur Einhaltung der Datenschutzvorschriften.

Mit der Änderung des Betriebsverfassungsgesetzes (BetrVG) durch das Betriebsrätemodernisierungsgesetz (in Kraft seit 18. Juni 2021) ist in der Frage Klarheit geschaffen worden, ob der Betriebsrat selbst als Verantwortlicher anzusehen ist.
Nach dem Wortlaut des § 79a Satz 2 BetrVG ist nunmehr klargestellt: Der Arbeitgeber ist der für die Verarbeitung Verantwortliche im Sinne des Art 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO). Den Be-

triebsrat trifft weiterhin die Pflicht zur Einhaltung der Datenschutzvorschriften. Unterstützung und gegebenenfalls auch Kontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten, der einerseits die Sensibilität der Tätigkeit des Betriebsrats zu beachten hat, andererseits aber auch dem Arbeitgeber gegenüber zur Aufgabenwahrnehmung verpflichtet ist. Dabei unterliegt er der Verschwiegenheit gegenüber dem Arbeitgeber hinsichtlich Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. Insoweit ist sichergestellt, dass die Wahrnehmung der Aufgaben durch den Betriebsrat insbesondere gegenüber den Beschäftigten durch den Arbeitgeber als Verantwortlichen nicht beeinträchtigt werden darf.
Da der Gesetzestext es nun eindeutig festlegt, ist der Betriebsrat nicht als eigenständig Verantwortlicher im Sinne des Art 4 Nr. 7 DS-GVO zu behandeln.

1.9 Interessenkollision zwischen der Funktion als Datenschutzbeauftragter und Personalrat?

Aus der Stellung als Datenschutzbeauftragter ergibt sich kein offensichtlicher Interessenkonflikt, der eine Mitwirkung im Hauptpersonalrat der obersten Dienstbehörde grundsätzlich ausschließt, wenn es sich um einen Datenschutzbeauftragten handelt, der Datenschutzbeauftragter einer dieser obersten Dienstbehörde untergeordneten öffentlichen Stelle ist. Um das Konzept einer unabhängigen Selbstkontrolle nicht zu konterkarieren, sollte allerdings Zurückhaltung in datenschutzrechtlich relevanten Fragen geübt werden, die Auswirkungen auf die Datenverarbeitung bei dem Verantwortlichen haben können, dessen Datenschutzbeauftragter das Mitglied ist.

Der Datenschutzbeauftragte einer öffentlichen Stelle in Thüringen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob seine Stellung als Datenschutzbeauftragter mit einer Mitgliedschaft im Hauptpersonalrat vereinbar sei, für den er beabsichtige zu kandidieren.
Der TLfDI teilte dem Datenschutzbeauftragten mit, dass die durch Art. 39 Abs. 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO) festgelegte Hauptaufgabe des Datenschutzbeauftragten darin bestehe, innerhalb der Organisation des Verantwortlichen die Aufsicht über die Einhaltung der datenschutzrechtlichen Regelungen zu führen.

Ein interner Datenschutzbeauftragter, der zugleich Teil des Verantwortlichen und mit ihm vertraglich verbunden ist, darf allerdings auch andere Aufgaben wahrnehmen, sofern dies gemäß Art. 38 Abs. 6 DS-GVO nicht zu einem Interessenkonflikt führt.
Ob und inwieweit ein Interessenkonflikt zwischen der Aufgabe des Datenschutzbeauftragten und der Mitgliedschaft im Personal- beziehungsweise Betriebsrat besteht, ist umstritten. Nach Ansicht des Bundesarbeitsgerichts (BAG) ist durch die bloße Mitgliedschaft des Datenschutzbeauftragten im Betriebsrat keine Interessenkollision ersichtlich, der eine grundsätzliche Inkompatibilität zwischen beiden Ämtern rechtfertigt (BAG, NZA 2011, 1036 Rn. 25; wobei das Gericht die Abwesenheit von Interessenkonflikten nach Bundesdatenschutzgesetz a.F. als eine Frage der Zuverlässigkeit betrachtet). Auch für das Landesarbeitsgericht Mecklenburg-Vorpommern ist die Mitgliedschaft im Betriebsrat grundsätzlich mit der Tätigkeit des Datenschutzbeauftragten vereinbar (NZA-RR, 2020, 291 Rn. 36 = Rn. 43 juris). Gleichwohl wird zur Vermeidung eines Rollenkonflikts allgemein Zurückhaltung empfohlen (Ehmann/Selmayr/Heberlein, DS-GVO, Art. 38 Rn. 24; Sydow/Helrich, DS-GVO, Art. 38 Rn. 78; Wolff/Brink/Moos, DS-GVO, Art. 38 Rn. 37).
Wie das BAG unter Geltung der DS-GVO ausführt, liegt ein Interessenkonflikt immer dann vor, wenn der Datenschutzbeauftragte seine eigene Tätigkeit kontrollieren muss (BAG, NJW 2020, 227 Rn. 25). Insofern kann sich ein Interessenkonflikt aus dem Umstand ergeben, dass der Personalrat als Teil des Verantwortlichen der Kontrolle durch den Datenschutzbeauftragten unterliegt. Ob dies der Fall ist, hängt allerdings von der konkreten Ausgestaltung des Mitbestimmungsrechts ab.
Der Datenschutzbeauftragte wollte für den Hauptpersonalrat kandidieren, der als Stufenvertretung gemäß § 53 Abs. 1 Thüringer Personalvertretungsgesetz (ThürPersVG) bei der obersten Dienstbehörde gebildet und nach § 82 Abs. 2 ThürPersVG beteiligt wird, wenn die Entscheidungskompetenz bei der obersten Dienstbehörde angesiedelt ist. Folglich liegen auch die Kontrollpflichten für den Hauptpersonalrat beim Datenschutzbeauftragten dieser Stelle, sofern sich Personalvertretung und Dienststelle nach § 80 Abs. 1 Satz 2 ThürPersVG auf einen gemeinsamen Datenschutzbeauftragten geeinigt haben.
Aus der Stellung als Datenschutzbeauftragter einer dieser obersten Dienstbehörde untergeordneten Behörde ergibt sich kein offensichtlicher Interessenkonflikt, der eine Mitwirkung im Hauptpersonalrat der

obersten Dienstbehörde grundsätzlich ausschließt. Um das Konzept einer unabhängigen Selbstkontrolle nicht zu konterkarieren, wurde empfohlen, als gewähltes Mitglied des Hauptpersonalrats Zurückhaltung bei der Entscheidung über datenschutzrechtlich relevante Fragen zu üben, die Auswirkungen auf die Datenverarbeitung bei dem Verantwortlichen haben können, dessen Datenschutzbeauftragter das Mitglied ist, um einen möglichen Anschein der Vermischung der verschiedenen Aufgaben zu vermeiden. So kann der Datenschutzbeauftragte sich dieser datenschutzrechtlichen Frage dann vornehmlich in seiner Rolle als Datenschutzbeauftragter des Verantwortlichen annehmen. Ob die Kandidatur erfolgreich gewesen war, ist dem TLfDI nicht bekannt.

1.10 Kurz, schnell und ungeschützt – Übermittlung von Impfzertifikaten per E-Mail

Impfzertifikate sind personenbezogene Gesundheitsdaten. Sie zählen zu den besonderen Kategorien von Daten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit Art. 4 Nr. 15 DS-GVO. Diese Daten unterliegen einem besonderen Schutz. Eine Übermittlung dieser Daten über unverschlüsselte E-Mail verstößt gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO. Insofern verstößt auch die Forderung, Impfzertifikate über unverschlüsselte E-Mail an das Gesundheitsamt zu übermitteln, ohne einen sicheren Übermittlungsweg (beispielsweise Ende-zu Ende-Verschlüsselung der E-Mail) anzubieten, gegen die datenschutzrechtlichen Vorgaben.

Im November 2021 beschwerte sich eine Bürgerin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Gesundheitsamt sie aufgefordert habe, ihr Impfzertifikat per E-Mail auf einen persönlichen dienstlichen Account eines Mitarbeiters des Gesundheitsamtes zu übersenden. Nachdem die betroffene Bürgerin ihre Bedenken zur Übersendung von Gesundheitsdaten auf unsicherem Weg über unverschlüsselte E-Mail an eine ihr unbekannte Person geäußert hatte, erhielt sie vom Gesundheitsamt die Möglichkeit, ihr Impfzertifikat persönlich im Amt vorzulegen. Der Mitarbeiter des Gesundheitsamtes behielt das Impfzertifikat der betroffenen Bürgerin mit ihrem Einverständnis ein.

Bei positiven und negativen Testergebnissen über das Vorliegen oder Nichtvorliegen einer Infektion mit COVID-19 handelt es sich um personenbezogene Gesundheitsdaten, das heißt besondere Kategorien von Daten im Sinne von Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 15 Datenschutz-Grundverordnung (DS-GVO). Für diese Daten gilt ein erhöhter Schutz und es ist weder zulässig, diese Daten auf unsicherem Weg über unverschlüsselte E-Mail zu übermitteln noch dies von betroffenen Personen alternativlos zu fordern. Die Forderung einer unverzüglichen Übermittlung von Testergebnissen durch das Gesundheitsamt war angesichts des Pandemiegeschehens Ende 2021 nachvollziehbar. Gleichwohl entband diese Forderung das Gesundheitsamt als Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO nicht davon, die Daten nach Art. 5 Abs. 1 Buchstabe f) DS-GVO vor dem Zugriff unbefugter Dritter durch geeignete Maßnahmen zu schützen, beispielsweise durch eine (Ende-zu-Ende-)Verschlüsselung der geforderten E-Mails. Zudem war nicht erforderlich, das Impfzertifikat der Beschwerdeführerin einzubehalten. Eine reine Vorlage des Zertifikats mit entsprechender Dokumentation wäre nach den gesetzlichen Vorgaben ausreichend gewesen, sodass die geforderte Übersendung per E-Mail und das Einbehalten des Impfzertifikats den Vorgaben zur Rechtmäßigkeit, Transparenz und zur Datenminimierung aus Art. 5 Abs. 1 Buchstabe a) DS-GVO und Art. 5 Abs. 1 Buchstabe c) DS-GVO zuwiderliefen.

Der TLfDI wies das Gesundheitsamt auf den Verstoß gegen die datenschutzrechtlichen Vorgaben hin und forderte Auskunft darüber, ob das Gesundheitsamt für die Übermittlung von Gesundheitsdaten eine Verschlüsselungstechnik angeboten und die Betroffenen auf den fehlenden Schutz ihrer personenbezogenen Daten bei unverschlüsselter Übermittlung hingewiesen hatte, welche Mitarbeiter Zugriff auf die unverschlüsselten Daten hatten und wie die personenbezogenen Gesundheitsdaten (Impfzertifikate) im Gesundheitsamt verarbeitet wurden.

Anfang März 2022 teilte das Gesundheitsamt mit, dass für die elektronische Übermittlung von personenbezogenen Daten und Impfzertifikaten an das Gesundheitsamt eine entsprechende Verschlüsselungstechnik angeboten wurde; der betreffende Mitarbeiter des Gesundheitsamtes habe die Beschwerdeführerin wider besseres Wissen zur Übersendung ihres Impfzertifikats mittels unverschlüsselter E-Mail aufgefordert. Zudem war nach Mitteilung des Gesundheitsamtes auch

der postalische Weg zur Datenübermittlung nicht grundsätzlich ausgeschlossen. Das Gesundheitsamt habe die Beschwerde und das Auskunftsersuchen des TLfDI zum Anlass genommen, den Mitarbeiter auf den datenschutzrechtlichen Verstoß seines Handelns hinzuweisen und ihn über die einzuhaltenden verschlüsselten Übermittlungswege per E-Mail belehrt. Weiterhin erörterte das Gesundheitsamt den Vorfall mit allen Mitarbeitern und belehrte diese nochmals eingehend zur Einhaltung des Datenschutzes.
Zur Verarbeitung der personenbezogenen Gesundheitsdaten teilte das Amt mit, dass die elektronisch verschlüsselt übermittelten Daten innerhalb eines gesicherten Netzwerkes an ein Sammelpostfach des Gesundheitsamtes übertragen würden. Hier wurden die Impfzertifikate durch eine zugriffsberechtigte Person der Abteilung Gesundheitsschutz im Netzlaufwerk des Gesundheitsamtes in einen lese- und schreibgeschützten Ordner zur Einsichtnahme durch den zuständigen Bearbeiter zwischengespeichert. Nach Einsichtnahme wurde in der Fachsoftware der Vermerk über den Impfstatus der betroffenen Personen einschließlich Impfdaten und Impfstoffname hinterlegt. Zusätzlich wurde eine analoge Kopie des (Impf-)Nachweises an die Fallakte geheftet und somit datenschutzrechtlich im Sinne von Art. 4 Nr. 2 DS-GVO gespeichert. Der TLfDI wies darauf hin, dass die analoge Speicherung gegen die Vorgabe aus Art. 5 Abs. 1 Buchstabe c) DS-GVO zur Datenminimierung verstieß, da die Daten bereits elektronisch erfasst waren. Daraufhin beendete das Gesundheitsamt die analoge Speicherung und teilte ergänzend mit, dass der lese- und schreibgeschützte Ordner, in dem die personenbezogenen Impfdaten und -zertifikate im Gesundheitsamt nur zwischengespeichert wurden und der gesamte Inhalt des Ordners Anfang April 2022 ebenfalls vollständig gelöscht wurden.
Zur elektronischen Speicherung teilte das Gesundheitsamt mit, dass die personenbezogenen Gesundheitsdaten der betroffenen Personen (Stammdaten wie Name und Adresse sowie Impfdaten, unter anderem Impfdatum, Impfstoff, Anzahl der Impfungen et cetera) auf Grundlage von § 16 Abs. 1 Infektionsschutzgesetz in der Software SORMAS gespeichert und gemäß § 630f Abs. 3 Bürgerliches Gesetzbuch für die Dauer von zehn Jahren aufbewahrt würden. Auf Nachfrage des TLfDI teilte das Gesundheitsamt mit, dass in der Software SORMAS der Impfstoffname, das Impfdatum und die Chargennummer des Impfstoffs nur als freiwillige Angaben der betroffenen Personen gespeichert würden.

Da die Beschwerdeführerin der Aufforderung zur unverschlüsselten Übermittlung ihrer personenbezogenen Gesundheitsdaten nicht gefolgt war und insofern einen möglichen Zugriff durch unbefugte Dritte selbst verhindert hat, konnte datenschutzrechtlich keine Verletzung des Schutzes personenbezogener Daten festgestellt werden. Gleiches ergab sich bei der datenschutzrechtlichen Prüfung der elektronischen Verarbeitungsvorgänge von personenbezogenen Gesundheitsdaten (insbesondere Impfzertifikaten) im Gesundheitsamt. Durch die Belehrung des Mitarbeiters, der die Beschwerdeführerin zur unverschlüsselten Datenübermittlung aufgefordert hatte und die datenschutzrechtliche Erörterung des Falles mit allen Mitarbeitern hat das Gesundheitsamt die organisatorischen und technischen Maßnahmen nach Art. 32 Abs. 1 DS-GVO ergriffen, um entsprechende Vorkommnisse in Zukunft zu vermeiden. Die Beschwerdeführerin wurde vom TLfDI entsprechend informiert.

1.11 3G am Arbeitsplatz – Speicherdauer

Nach Auffassung des TLfDI war es für die Erfüllung der Überprüfungspflicht grundsätzlich nicht erforderlich, die 3G-Nachweisdaten der Beschäftigten über den täglichen Nachweis hinaus aufzubewahren. Lag eine Einwilligung vor, konnte der Nachweis bis zum Ablauf der Sechsmonatsfrist nach § 28b Abs. 3 Satz 9 IfSG aufbewahrt oder gespeichert werden, längstens jedoch für die Dauer der betrieblichen Zugangsbeschränkung.

Auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) musste am Anfang des Berichtszeitraumes die zum Nachweis der betrieblichen Zugangsbeschränkungen („3G am Arbeitsplatz“) nach § 28b Abs. 3 Infektionsschutzgesetz (IfSG) dokumentierten personenbezogenen Daten für Kontrollzwecke des Gesundheitsamtes aufbewahren. Das zuständige Gesundheitsamt hielt es für erforderlich, diese Daten vier Wochen aufzubewahren, um seiner nach den Gesetzen bestehenden Überwachungstätigkeit nachkommen zu können.
Dabei verwies das Gesundheitsamt auf die Aufbewahrungsfrist, die für die Durchführung der infektionsschutzrechtlichen Zugangsbeschränkungen in der Thüringer SARS-CoV-2-Infektionsschutz-Maßnahme-Verordnung (ThürSARS-CoV-2-IfS-MaßnVO) enthalten war (§ 13 Abs. 5 ThürSARS-CoV-2-IfS-MaßnVO). Hierzu machte der

TLfDI deutlich, dass für betriebliche Zugangsbeschränkungen die Regelungen des § 28b Abs. 1 und 3 Infektionsschutzgesetz (IfSG) Anwendung finden. Es handelt sich um eine Maximalfrist, sodass die „datenschutzgerechte“ Löschung oder Vernichtung nach dem als Richtschnur zu beachtenden Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e) Datenschutz-Grundverordnung [DS-GVO]) früher erfolgen muss, sofern dies möglich ist (so auch die Begründung zum Verordnungsentwurf, Seite 21). Gleiches gilt für die Sechsmonatsfrist des § 28b Abs. 3 Satz 9 IfSG.
Nach Auffassung des TLfDI war es für die Erfüllung der Überprüfungspflicht grundsätzlich nicht erforderlich, die 3G-Nachweisdaten der Beschäftigten über den täglichen Nachweis hinaus aufzubewahren. Nur wenn der betriebliche Umsetzungsaufwand außer Verhältnis zu einer täglichen Überprüfung gestanden hätte, wäre im Einzelfall die Erforderlichkeit einer längerfristigen Speicherung oder Aufbewahrung der 3G-Nachweisdaten zu begründen gewesen.
Dabei ist zwischen der vorgeschriebenen Dokumentation der täglich durchgeführten Zugangskontrolle und dem Wunsch der Beschäftigten auf Hinterlegung ihrer Angaben zum Impf- oder Genesungsstatus zu unterscheiden. Liegt eine Einwilligung vor, kann der Nachweis bis zum Ablauf der Sechsmonatsfrist (§ 28b Abs. 3 Satz 9 IfSG) aufbewahrt oder gespeichert werden, längstens jedoch für die Dauer der betrieblichen Zugangsbeschränkung.
Diese Rechtsauffassung hatte der TLfDI auch in den FAQ zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie auf seiner Homepage veröffentlicht.
Die Argumentation des Gesundheitsamtes, dass bei einer arbeitstäglichen Löschung des 3G-Nachweises eine Überprüfung der vom Arbeitgeber durchzuführenden Nachweiskontrollen nicht gewährleistet werden könne, überzeugte nicht. Zum einen hatte das Bundesministerium für Arbeit und Soziales von der Möglichkeit des § 28b Abs. 6 Satz 2 Nr. 2 IfSG, durch Rechtsverordnung die Ausgestaltung der Dokumentationspflichten zu präzisieren, keinen Gebrauch gemacht. Zum anderen führte das Ministerium in seinen Fragen und Antworten zum betrieblichen Infektionsschutz aus, dass im Infektionsschutzgesetz keine Mindestaufbewahrungsfrist vorgesehen ist, sodass es bei einer eventuellen behördlichen Kontrolle genügt, die Kontrolldokumentation für den aktuellen Tag vorzulegen.

Auch für Ermittlungen zu Übertragungen im betrieblichen Umfeld sowie zum Ausschluss beziehungsweise zur Unterbrechung von Infektionsketten sah der TLfDI keine Notwendigkeit einer längeren Aufbewahrungsfrist. Hierbei ist zu beachten, dass nach dem Zweckbindungsgrundsatz des Art. 5 Abs. 1 Buchstabe b) DS-GVO personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und in einer mit diesen Zwecken zu vereinbarenden Weise verarbeitet werden dürfen. Deshalb können die nach § 28b Abs. 3 IfSG erhobenen Daten auch nur für Zwecke der Einhaltung der 3G-Regel im Rahmen des betrieblichen Infektionsschutzes dokumentiert werden. Mit Blick auf den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO) genügt es, wenn zum Zweck einer Kontrolle der betrieblichen Zugangsbeschränkung das Vorhandensein eines gültigen Nachweises („ob“) und, soweit die Erforderlichkeit begründet werden kann, die Art und gegebenenfalls die Gültigkeitsdauer des vorgelegten Nachweises („welcher“) dokumentiert wird. Durch die Dokumentation sollten Infektionseinträge im Betrieb und damit verbundene Personalausfälle durch Erkrankung und Quarantäne wirksam reduziert werden (Gesetzesbegründung, BT-Drucksache 20/89, Seite 18), weshalb die Daten zum Impf-, Sero- und Teststatus auch zur Anpassung des betrieblichen Hygienekonzepts auf Grundlage der Gefährdungsbeurteilung gemäß den §§ 5 und 6 des Arbeitsschutzgesetzes verwendet werden durften. Es war nicht ersichtlich, inwieweit die im Rahmen der betrieblichen Zugangskontrolle erhobenen Daten für eine wirksame Kontaktnachverfolgung überhaupt geeignet sind. Hierzu wurde das Gesundheitsamt um fachliche Erläuterung gebeten, die aber nicht erfolgte. Daher blieb es bei der oben dargestellten Bewertung des TLfDI, nach der die Nachweise jeweils spätestens am Folgetag zu löschen waren, außer in den Fällen, in denen eine Einwilligung der Beschäftigten vorlag.

1.12 Entscheidung des BVerwG: Anspruch auf unentgeltliche Kopien von Prüfungsarbeiten

Das Bundesverwaltungsgericht hat entschieden, dass Absolventen der zweiten juristischen Staatsprüfung gemäß Art. 15 Abs. 1 und Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 der Datenschutzgrundverordnung (DS-GVO) einen Anspruch auf die Anfertigung unentgeltlicher Kopien gegenüber dem jeweiligen Landesjustizprüfungsamt haben.

Die im Datenschutzrecht bereits oft kontrovers diskutierte Frage, ob Absolventen der zweiten juristischen Staatsprüfung einen Anspruch darauf haben, dass ihnen das Landesjustizprüfungsamt unentgeltlich eine Kopie der von ihnen angefertigten Aufsichtsarbeiten mitsamt den zugehörigen Prüfergutachten zur Verfügung stellt, wurde in einem Urteil vom Bundesverwaltungsgericht (BVerwG) in Leipzig am 30. November 2022 entschieden (BVerwG 6 C 10.21). Der Anspruch wurde durch das BVerwG bejaht!
Nach Art. 15 Abs. 1 Datenschutzgrundverordnung (DS-GVO) hat die betroffene Person unter anderem das Recht auf Auskunft über ihre personenbezogenen Daten. Gemäß Art. 15 Abs. 3 Satz 1 DS-GVO kann sie von dem Verantwortlichen die Überlassung einer Kopie der personenbezogenen Daten verlangen, die Gegenstand der Verarbeitung sind. Aus Art. 12 Abs. 5 Satz 1 in Verbindung mit Art. 15 Abs. 3 Satz 2 DS-GVO ergibt sich, dass die erste Kopie unentgeltlich zur Verfügung gestellt werden muss.
Mit seinem Urteil vom 20. Dezember 2017 hatte bereits der Gerichtshof der Europäischen Union (EuGH, C-434/16) geklärt, dass schriftliche Prüfungsleistungen in einer berufsbezogenen Prüfung und die Anmerkungen der Prüfer dazu wegen der in ihnen jeweils enthaltenen Informationen über den Prüfling insgesamt – das heißt letztlich Wort für Wort – personenbezogene Daten des Prüflings darstellen.
Damit wurde nunmehr durch ein oberstes Gericht der Bundesrepublik Deutschland eindeutig festgestellt, dass ein Prüfling das Recht auf Erhalt einer vollständigen Kopie der schriftlichen Prüfungsarbeiten und der zugehörigen Prüfergutachten hat. Das zuständige Landesprüfungsamt muss somit dem Prüfling diese Kopien unentgeltlich zur Verfügung stellen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit wird im nächsten Tätigkeitsbericht die Auswirkungen dieser Entscheidung für das Ausmaß des Auskunftsanspruchs auch in anderen Fallkonstellationen ausleuchten.

1.13 Verwendung anonymisierter Daten zu Forschungszwecken

Anonymisierte Daten fallen mangels Personenbezug nicht unter die DS-GVO. Einer Nutzung für wissenschaftliche Zwecke stehen dann keine datenschutzrechtlichen Hindernisse entgegen.

Ein Studierender wandte sich mit einer Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Im Rahmen einer Bachelorarbeit sollten Daten von Patienten einer Thüringer Klinik zur wissenschaftlichen Auswertung verwendet werden, die standardisiert und anonymisiert über Fragebögen erhoben wurden.

Auf die Anfrage, ob dies datenschutzrechtlich zulässig sei, hat der TLfDI zunächst darauf hingewiesen, dass Patientendaten, soweit sie lediglich in anonymisierter Form vorliegen, also sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, nicht zu den besonderen Kategorien von Daten nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) zählen, für die ein erhöhter Schutz gilt. Vielmehr fallen anonymisierte Daten mangels Personenbezugs oder -beziehbarkeit nicht unter die DS-GVO. Sollten die Angaben allerdings lediglich pseudonymisiert worden sein, also beispielsweise über eine vergebene Kennung oder über weitere Angaben eine Zuordnung zu einer bestimmten Person zulassen – vergleiche Art. 4 Nr. 5 DS-GVO – , handelt es sich um personenbezogene Daten, auf die die DS-GVO Anwendung findet und es müsste bereits mit der Erhebung mittels Fragebogen auch der Zweck der Datenerhebung im Sinne von Art. 5 Abs. 1 Buchstabe b) DS-GVO mitgeteilt worden sein. Im konkreten Fall also die Nutzung für eine Bachelor-Arbeit als wissenschaftliche Arbeit.

Eine Verarbeitung der Gesundheitsdaten kann nach Art. 9 Abs. 2 Buchstabe g) DS-GVO außerdem auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaates erfolgen, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht. Art. 89 DS-GVO als Unionsrecht sieht Garantien und Ausnahmen in Bezug auf die Verarbeitung zu wissenschaftlichen Zwecken vor. Bei der Verarbeitung von personenbezogenen Daten durch Forschungseinrichtungen im öffentlichen Bereich sind die Anforderungen nach § 28 Thüringer Datenschutzgesetz (ThürDSG) zu beachten. Nach § 28 Abs. 3 ThürDSG sind die personenbezogenen Daten, sobald dies nach dem Forschungszweck möglich ist, dergestalt zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen

Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (anonymisieren).
Es stellte sich heraus, dass der Studierende noch in der Klinik beschäftigt war und die Daten erst noch in die anonymisierten Fragebögen übernommen werden mussten.
Gegen die Anonymisierung der Patientendaten für spätere Forschungszwecke auf der Grundlage des § 27 Bundesdatenschutzgesetz durch in einer Klinik beschäftigte Studierende bestanden keine Bedenken, sofern sie aufgrund ihrer Beschäftigung nach dem Rollen- und Zugriffsrechtekonzept zugriffsberechtigt sind. Zur Nutzung für wissenschaftliche Zwecke riet der TLfDI darüber hinaus, den/die Datenschutzbeauftragte/n der Klinik vor Ort einzubeziehen.

1.14 Newsletterversendung und Werbesendungen ohne Einwilligung oder Vorliegen der Voraussetzungen des UWG

Die Versendung von Werbung per E-Mail ist für die Verantwortlichen an strenge Voraussetzungen geknüpft. Ausnahmsweise ist es aufgrund von § 7 Abs. 3 UWG in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO jedoch möglich, an Bestandskunden eines Verantwortlichen unter bestimmten Voraussetzungen E-Mail-Werbung zu versenden. Ohne das positive und kumulative Vorliegen der Voraussetzungen des § 7 Abs. 3 UWG bedarf es aber für die Nutzung von E-Mail-Adressen zu Werbezwecken (wie zum Beispiel bei Newslettern) grundsätzlich einer ausdrücklichen Einwilligung.

Während des Berichtszeitraumes erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zahlreiche Beschwerden über die Versendung von Newslettern und Produktwerbungen per E-Mail diverser Unternehmen. Die betroffenen Personen rügten in diesen Fällen oftmals, dass sie nach einer Bestellung von Waren oder Dienstleistungen E-Mail-Werbung erhalten, obwohl sie zu keinem Zeitpunkt eine Einwilligung in den Newsletterversand gegeben haben.
Nicht in allen Fällen führt dieser Umstand jedoch zu einer widerrechtlichen Datenverarbeitung im Rahmen der E-Mail-Werbung. Nachfolgend sollen daher die rechtlichen Voraussetzungen der Werbemaßnahmen näher beleuchtet werden.

Als rechtliche Grundlage für die Versendung von Werbung können sich die Verantwortlichen grundsätzlich auf ihr berechtigtes Interesse nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der Datenschutz-Grundverordnung (DS-GVO) berufen. Danach wird das Interesse eines Verantwortlichen, für seine Produkte und Dienstleistungen Werbung mit dem Ziel zu machen, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern, als ein berechtigtes Interesse angesehen. Dies ergibt sich auch aus Erwägungsgrund 47 der DS-GVO. Im Rahmen der Interessenabwägung ist im konkreten Einzelfall zwischen den Interessen des Verantwortlichen beziehungsweise Dritten und der betroffenen Person abzuwägen.
Dabei ist hier noch eine Besonderheit außerhalb des Datenschutzrechtes zu beachten, welches die Interessenabwägung beeinflusst. Die Werbung mittels E-Mail ist auch im Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt und ist grundsätzlich nur zulässig, wenn vorab eine Einwilligung des Empfängers gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO eingeholt wurde, da nach § 7 Abs. 2 Nr. 3 UWG jede Werbung unter Verwendung elektronischer Post ohne vorherige ausdrückliche Einwilligung des Empfängers eine unzumutbare Belästigung darstellt. Jedoch enthält der § 7 UWG auch einen Ausnahmetatbestand in seinem Absatz 3. Wenn E-Mail-Adressen unmittelbar von den betroffenen Personen im Rahmen einer Vertragsbeziehung (Bestandskunden) erhoben wurden, überwiegen schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in der Regel dann nicht, wenn die in § 7 Abs. 3 UWG enthaltenen Vorgaben für elektronische Werbung eingehalten werden.
Soll für die Direktwerbung die Rechtsgrundlage des § 7 Abs. 3 UWG in Betracht kommen, müssen dessen Voraussetzungen positiv und vor allem kumulativ vorliegen. Nur dann kann der Versand von E-Mail-Werbung auf § 7 Abs. 3 UWG in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO als Rechtsgrundlage gestützt werden und eine Einwilligung ist nicht erforderlich.
Zunächst muss es sich bei dem Empfänger um einen Bestandskunden des Verantwortlichen handeln. Das heißt, dass der Verantwortliche die E-Mail-Adresse des Empfängers im Rahmen eines Verkaufes einer Ware oder Dienstleistung von ihm erhalten haben muss. Zwischen dem Empfänger und dem Verantwortlichen muss daher ein Vertrags-

verhältnis bestanden haben oder bestehen. Ein vorvertragliches Verhältnis reicht dazu nicht aus. Auch eine ausgeführte Bestellung als „Gast“ führt zu einem Vertragsverhältnis.
Weiterhin darf der Empfänger der Verwendung seiner E-Mail-Adresse für Werbezwecke zum Zeitpunkt der Versendung nicht widersprochen haben. Auch muss der Kunde bei jeder Verwendung der Adresse klar und deutlich durch den Versender darauf hingewiesen werden, dass er der Verwendung jederzeit kostenlos widersprechen kann. Dies erfolgt in der Regel durch einen Hinweis am Ende des Werbeschreibens.
Als letzte Voraussetzung legt § 7 Abs. 3 UWG fest, dass die E-Mail-Adressen von Bestandskunden seitens des Unternehmers lediglich zur Werbung für eigene ähnliche Waren oder Dienstleistungen genutzt werden dürfen. Anhand welcher genauen Kriterien die Bestimmung der Waren- und Dienstleistungsähnlichkeit zu erfolgen hat, ist teilweise verschieden. „Ähnlich“ wird seitens der Rechtsprechung aber sehr eng ausgelegt um den Adressaten vor ungebetener Werbung zu schützen. Das OLG Thüringen (Urteil vom 21. April 2010, Az. 2 U 88/10) führt dazu aus, dass sich die Ähnlichkeit auf die bereits gekauften Waren beziehen und dem gleichen typischen Verwendungszweck oder Bedarf des Kunden entsprechen muss; gegebenenfalls ist es noch zulässig, Zubehör oder Ergänzungswaren zu bewerben. Davon ist regelmäßig auszugehen, wenn die Produkte austauschbar sind oder dem gleichen oder einem ähnlichen Bedarf oder Verwendungszweck dienen.
Daher ist grundsätzlich zwischen der Übersendung von Newslettern und der gezielten Produktwerbung per E-Mail nach § 7 Abs. 3 UWG zu unterscheiden. Ein Newsletter bewirbt die gesamte Produktpalette des Verantwortlichen und wird in bestimmten Zeitabständen versendet. Für die Versendung von Newslettern muss der Verantwortliche daher bei den Empfängern eine Einwilligung nach Art. 4 Nr. 11 DS-GVO in Verbindung mit Art. 7 Abs. 2, 3 DS-GVO einholen und gegebenenfalls auch nachweisen können, Art. 7 Abs. 1 DS-GVO. Für Newsletter steht daher als Rechtsgrundlage allein der Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, also die Einwilligung zur Verfügung.
Die Einwilligung muss dabei ausdrücklich, informiert und freiwillig unter dem Hinweis auf das jederzeitige Widerrufsrecht gemäß Art. 7 DS-GVO erfolgen. Diese Einwilligung muss vom Verantwortlichen auch dokumentiert werden, um seiner Rechenschaftspflicht nachzukommen, Art. 5 Abs. 2 DS-GVO.

Im Rahmen der gezielten E-Mail-Werbung im Rahmen des § 7 Abs. 3 UWG ist der Zweck der E-Mail-Werbung außerdem gemäß Art. 13 Abs. 1 Buchstabe c) DS-GVO den betroffenen Personen bei der Datenerhebung transparent darzulegen. Zudem muss der Verantwortliche nachweisen können, dass es sich bei der zu Werbezwecken verwendeten E-Mail-Adresse um die Adresse eines Bestandskunden handelt, Art. 5 Abs. 2 DS-GVO.

1.15 Gastzugang im Online-Handel

Neben der Möglichkeit der Einrichtung eines fortlaufenden Kundenkontos muss der Verantwortliche den Kunden, die keine dauerhafte Geschäftsbeziehung eingehen wollen oder eine Verarbeitung von nicht zur Geschäftsabwicklung benötigten Daten ablehnen, regelmäßig einen Gastzugang ermöglichen.

Auch in diesem Berichtszeitraum erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wieder mehrere Beschwerden, in denen darauf hingewiesen wurde, dass es bei verschiedenen Anbietern im Bereich des Online-Handels nicht möglich sei, ohne eine Registrierung als Kunde zu bestellen. Da es sich dabei nicht nur um ein Problem in Thüringen handelt, hat sich der TLfDI verstärkt dafür eingesetzt, dass dieses Thema in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zur Diskussion gestellt wird. Als Folge wurde am 24. März 2022 ein Beschluss mit Hinweisen zum datenschutzkonformen Online-Handel erlassen. Dieser ist unter dem folgenden Link zu finden: https://www.datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf.
Der wesentliche Inhalt des Beschlusses soll an dieser Stelle erläutert werden.
Verantwortliche, die Waren oder Dienstleistungen im Online-Handel anbieten, müssen ihren Kunden unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kundenkonto) zur Verfügung stellen, grundsätzlich einen Gastzugang (Online-Geschäft ohne Anlegen eines fortlaufenden Kundenkontos) für die Bestellung bereitstellen.
Nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist nur die Verarbeitung der personenbezogenen Daten zulässig, die für die Erfüllung des

einzelnen Vertrages erforderlich sind. Bei einer erstmaligen Bestellung kann der Verantwortliche nicht per se unterstellen, dass er Daten von Kunden für mögliche, aber ungewisse zukünftige Geschäfte auf Vorrat speichern darf. Für die Einrichtung eines fortlaufenden Kundenkontos ist eine entsprechende bewusste Willenserklärung der Kunden erforderlich. Ein solches fortlaufendes Kundenkonto wird unter Vergabe von Zugangsdaten (zum Beispiel Benutzername/Passwort) eingerichtet, um sich gegenüber dem Verantwortlichen eindeutig zu identifizieren. Kunden können damit auf ein bei dem Verantwortlichen geführtes Kundenkonto selbst und aktiv zugreifen, um gegebenenfalls ihre Daten zu ändern oder Bestellungen zu prüfen. Fortlaufende Kundenkonten werden über den erstmaligen Geschäftsabschluss hinaus im Aktivdatenbestand gepflegt. Sie dienen den Kunden zur vereinfachten wiederkehrenden Bestellmöglichkeit ohne die nochmalige Eingabe aller personenbezogenen Daten. Darüber hinaus kann ein fortlaufendes Kundenkonto eine Bestell- oder Geschäftshistorie vorsehen, die dem Verantwortlichen eine Auswertung zur Profilbildung und für Werbezwecke ermöglicht.

Damit eine für die Einrichtung eines fortlaufenden Kundenkontos erforderliche Einwilligung nicht gegen die in Art. 7 Abs. 4 DS-GVO erwähnte Konditionalität verstößt, müssen die Kunden im Online-Shop auch die gleichen Angebote auf anderem gleichwertigen Wege als über das fortlaufende Kundenkonto bestellen können (vergleiche Rn. 37f. der Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des Europäischen Datenschutzausschusses vom 4. Mai 2020). Konditionalität liegt dann vor, wenn die Erfüllung eines Vertrages oder die Erbringung einer Leistung an die Einwilligung zu einer Verarbeitung personenbezogener Daten geknüpft ist, die für die Erfüllung des Vertrages nicht notwendig sind. Gleichwertig ist eine Bestellmöglichkeit immer dann, wenn keinerlei Nachteile entstehen, also Bestellaufwand und Zugang zu diesen Möglichkeiten, wie bei einem Gastzugang, denen eines laufenden Kundenkontos entsprechen und technisch organisatorische Maßnahmen getroffen werden, die ein angemessenes Datenschutzniveau gewährleisten.

Wenn in einem fortlaufenden Kundenkonto die über die Kontaktdaten hinausgehenden personenbezogenen Daten, gegebenenfalls einschließlich der Vertragsdaten der Bestellungen, für Werbezwecke (Profiling der Kundenhistorien, Zusammenführung mit Daten aus anderen Quellen) ausgewertet und verarbeitet werden sollen, sind darauf

bezogen Einwilligungen der Kunden nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO einzuholen. Die Auswertung stellt eine Verarbeitung dar, die über die bloße Einrichtung und Führung eines fortlaufenden Kundenkontos hinausgeht. Die Einwilligung zur Einrichtung und Führung des fortlaufenden Kundenkontos deckt damit nicht automatisch auch dessen Auswertung ab.
Für Kunden, die keine dauerhafte Geschäftsbeziehung eingehen wollen oder eine Verarbeitung von nicht zur Geschäftsabwicklung benötigten Daten ablehnen, ist daher regelmäßig ein Gastzugang zu ermöglichen. Ein solcher Zugang verzichtet auf Registrierungs- beziehungsweise Zugangsdaten (zum Beispiel Benutzername/Passwort) für eine erneute Nutzung. Über diesen Zugang dürfen nur die zur Durchführung des Vertrages und zur Erfüllung gesetzlicher Pflichten erforderlichen personenbezogenen Daten und Informationen der Kunden erfasst werden. Nach Vertragserfüllung nicht mehr benötigte Daten müssen gemäß Art. 17 Abs. 1 Buchstabe a) DS-GVO unverzüglich gelöscht werden. Ein Zugriff der Kunden auf die Daten oder das Hinzuspeichern von weiteren Daten durch die Verantwortlichen sind bei einem Gastzugang nicht vorgesehen.

1.16 Cookies: Was ist das? Was tun sie?

Cookies („Kekse“) sind kurze „Text-Schnipsel“, die eine vom Nutzer besuchte Webseite an dessen Browser sendet und die auf dem Rechner des Nutzers gespeichert werden. Alternativ wird der „Text-Schnipsel“ im Browser des Nutzers von einem Java Script erzeugt. Dort sammelt er für den Webseitenbetreiber Informationen, wie zum Beispiel Daten zur Technik, Funktionalität, Sicherheit, Personalisierung, zu Analysezwecken und für Werbung.

Cookies sind aus datenschutzrechtlicher Sicht nicht per se schlecht oder „böse“.
Doch wer kennt es nicht: Bei jedem Öffnen einer Webseite öffnet sich zunächst ein sogenanntes Cookie-Banner mit der Frage zur Einwilligung oder Ablehnung zur Datenverarbeitung an den Besucher der Webseite, bevor man an den eigentlichen Inhalt der Webseite kommt. Dabei treffen Menschen tagtäglich genügend Entscheidungen und fühlen sich daher eher genervt, wenn sie „nur mal schnell“ auf einer Webseite etwas lesen oder bestellen wollen. Das verleitet in unzähli-

gen Fällen dazu, einfach allem zuzustimmen, um endlich an das eigentliche Ziel, nämlich den Inhalt der Webseite zu gelangen. Viele wissen dabei nicht, in was sie da eigentlich einwilligen und welche Risiken solche dem ersten Anschein nach harmlosen Einwilligungen haben können. Dabei ist es doch wichtig, sich genau darüber zu informieren, welche Informationen man über sich an den Seitenbetreiber, Drittdienste und damit oftmals fremde Firmen weitergibt. Denn eines ist gewiss: Das Internet oder besser der Empfänger dieser Daten vergisst vorerst einmal nichts.

Hier ein paar Einsatzbeispiele, welche Informationen so ein Cookie sammeln kann:

a) eine Nummer, über die der Rechner beziehungsweise das Handy wiedererkennbar wird (IP-Adresse – wird zur Personalisierung bei Onlineshops oder Onlinebanking benötigt, hier ist es technisch notwendig),
b) die Webseitenadresse auf die sich das Cookie bezieht,
c) technische Einstellungen wie Sprache, Schriftgröße, Bildschirmeinstellung
(dient zur Erleichterung für den Webseitenbesucher und wird als technisch notwendig angesehen)
d) Meta-Daten wie das Ablaufdatum eines Cookies sowie der Adresspfad und die dazugehörigen Sicherheitsspezifikationen,
e) Zeit, die auf der Webseite oder ihren Unterseiten verbracht wird (dient zu Analysezwecken und bedarf der Einwilligung),
f) besuchte Unterseiten
(diese Information wird in der Regel zu Analyse- und Marketingzwecken genutzt und ist somit einwilligungspflichtig).

Viele Webseitenbetreiber gehen davon aus, dass Cookies für Werbetracking und Fingerprinting entscheidend zum geschäftlichen Erfolg beitragen und somit sich die Rechtmäßigkeit der Datensammlung mit dem Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) („dem berechtigten Interesse des Verantwortlichen oder eines Dritten“) vereinbaren lässt. In der Praxis zeigt sich das durch fehlende Cookie-Banner oder Cookie-Banner, auf denen die Nutzer (ohne Granularität in den Verarbeitungszwecken der Datenverarbeitung) nur zustimmen können. Diese Sichtweise greift jedoch zu kurz. Denn in Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO heißt es weiter, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen

Person um ein Kind handelt.“ Und genau hier setzt der Gesetzgeber sehr enge Grenzen für verantwortliche Webseitenbetreiber und fordert für technisch nicht erforderliche Cookies, also solche, die für den Betrieb einer Webseite nicht unbedingt benötigt werden, die Einholung einer wirksamen Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO der betroffenen Person zum Schutz ihrer Daten mit dem Ziel, dass sie die Hoheit darüber behält.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich dem Thema in den letzten Jahren sehr intensiv gewidmet und für Anbieter von Telemedien eine „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien), Version 1.1“ herausgegeben. Hier finden sich weitere nützliche Informationen. Die Orientierungshilfe ist abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf.
Bei Fragen hierzu können Sie sich gern an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden. Dieses Angebot richtet sich insbesondere an Verantwortliche, sprich Webseitenbetreiber mit Sitz in Thüringen. Diese tragen nämlich die Verantwortung und haften für alles, was auf ihrer Webseite passiert und müssen im Falle von Beschwerden gegenüber der Aufsichtsbehörde Rechenschaft ablegen können (Art. 5 Abs. 2 Datenschutz-Grundverordnung).

1.17 SDM V3.0

Die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer 104. Konferenz im November 2022 die dritte Version des SDM beschlossen und veröffentlicht. Neu betrachtet wurden unter anderem die Verarbeitungstätigkeiten und die Risiken für Betroffene.

Mit dem Standard-Datenschutzmodell (SDM) wird eine Methode bereitgestellt, mit der Verantwortliche und Aufsichtsbehörden bei der Entwicklung, bei der Datenschutzberatung und bei der Prüfung von Datenverarbeitungen beurteilen können, ob personenbezogene Daten

datenschutzkonform verarbeitet werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete bereits mehrfach in seinen Tätigkeitsberichten darüber.
Die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer 104. Konferenz im November 2022 die Version 3.0 des SDM beschlossen und veröffentlicht. In der nun aktuellen Version wurden insbesondere die Kapitel „Verarbeitungstätigkeiten“ und „Risiken für Betroffene“ überarbeitet beziehungsweise ergänzt, um der Datenschutz-Grundverordnung (DS-GVO) besser gerecht zu werden.
Bezüglich der „Verarbeitungstätigkeiten“ wurde die „Aufbereitung einer Verarbeitungstätigkeit in Vorgänge oder in Phasen eines Datenlebenszyklus“ beleuchtet. Um eine Verarbeitungstätigkeit datenschutzrechtlich zu untersuchen wird empfohlen, diese in relevante Teilprozesse zu zerlegen. Eine Verarbeitung beginnt mit dem Erhebungszusammenhang, gefolgt von der Nutzung, und sie endet beim Löschen beziehungsweise Vernichten von Daten. Das SDM geht nunmehr von neun Teilprozessen aus und ordnet diese auch tabellarisch den Begriffsbestimmungen gemäß Art. 4 Nr. 2 DS-GVO neu zu. Auch wurden die Phasen eines Datenlebenszyklus besser dargestellt und die Grafik „SDM-Würfel“ überarbeitet, um alle wesentlichen Risiken einer Verarbeitung auf einen Blick erfassen und diese analysieren zu können.
Hinsichtlich der Risiken für Betroffene wurden nunmehr aus technischer Sicht vier Risikostufen definiert. Im Unterschied zum allgemeinen Risikomanagement sowie zum Risikomanagement in der Informationssicherheit besteht im Bereich des Datenschutzes grundsätzlich die Pflicht, die durch die Verarbeitung personenbezogener Daten entstehenden Risiken mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen auf ein unbedingt erforderliches Schutzniveau zu reduzieren.
Damit wird für Anwender des SDM die Umsetzung ihrer Pflichten aus der DS-GVO erleichtert. Die SDM-Version 3.0 wurde veröffentlicht unter:
https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSK-BeschluessePositionspapiere/104DSK_SDM-3-0.pdf?__blob=publicationFile&v=2.

1.18 Verbotene Tricks von Anbietern von Sozialen Medien

Der Europäische Datenschutzausschuss hat im März 2022 Leitlinien für Entwickler, Anbieter und Nutzer von Social-Media-Plattformen mit praktischen Empfehlungen zur Bewertung und Vermeidung von gegen die DS-GVO verstoßenden „dunklen Mustern“ auf Benutzeroberflächen von sozialen Medien verabschiedet. Diese gilt es zukünftig zu beachten.

Der Europäische Datenschutzausschuss (EDSA) veröffentlicht regelmäßig Leitlinien, die als Auslegungshilfen beziehungsweise Umsetzungshilfen zu einzelnen Themen der Datenschutz-Grundverordnung (DS-GVO) dienen sollen. Am 14. März 2022 hat der EDSA in seiner 62. Sitzung die Leitlinien zu „Dark patterns“ bei der Oberflächengestaltung sozialer Netzwerke angenommen (aktueller Titel „Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them)“. Diese Leitlinien wurden im Februar 2023 leicht überarbeitet, sind derzeit aber nach wie vor nur in englischer Fassung auf dem Webauftritt des Europäischen Datenschutzausschusses (EDSA – englisch: European Data Protection Board-EDPB) abrufbar (https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf).
Unter „Dark patterns“ sind Benutzer-Oberflächen zu verstehen, durch die Nutzer aufgrund des Designs und der Gestaltung möglicherweise unbewusste, unbeabsichtigte und möglicherweise schädigende Entscheidungen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten treffen. Dadurch werden ihr Verhalten und ihre Fähigkeit, ihre Daten effektiv zu schützen, wesentlich beeinträchtigt. Mit „Dark patterns“ werden Personen, die auf sozialen Netzwerken aktiv sind, häufig dazu bewegt, mehr Daten über sich preiszugeben, als sie das eigentlich möchten; oder sie werden davon abgehalten, ihre Betroffenenrechte auszuüben.
Mit den Leitlinien gibt der EDSA praktische Empfehlungen, wie man solche „Dark patterns“ erkennen und ihnen auch entgegenwirken kann. Da die Leitlinien nur auf Englisch verfügbar und umfangreich sind, soll an dieser Stelle auf Beispiele von schädlichem Verhalten von Anbietern von sozialen Medien hingewiesen werden:

- Ständig wiederholte Meldungen, sein Profil zu vervollständigen, ohne die Möglichkeit zu haben, die Meldungen abzuschalten.

- Falschinformation, dass bestimmte Daten „notwendig“ sind, um eine Information zu erhalten (Beispiel: Angabe einer Telefonnummer, um dem Nutzer dann einen Link per SMS zum App-Store schicken zu können, was mit der ursprünglichen Information nichts zu tun hat).
- Emotionale Beeinflussung: Etwas ist sehr schnell möglich (zum Beispiel ein Nutzer-Profilbild) und hat einen großen Nutzen für den Nutzer; etwas NICHT zu machen wäre gefährlich oder bringt Nachteile und so weiter.
- Vor dem Löschen des Accounts werden die Konsequenzen drastisch dargestellt, um den Nutzer vom Löschen abzuhalten.
- Behinderungstaktik: Eine Funktion zu deaktivieren, dauert länger und ist viel umständlicher als die Funktion zu aktivieren (zum Beispiel die Freigabe von Daten mit einem Klick, aber Nicht-Freigabe wird durch langen Nachfrageprozess behindert).
- „Sichtbares verstecken“: bedeutet, Inhaltselemente wie Schaltflächen, Links zu Informationen sind grafisch so gestaltet, dass diese einfach übersehen werden können und nicht gleichberechtigt angezeigt werden.
- Überspringen von Detaileinstellungen, welche nicht datenminimal sind: Hier werden dem Nutzer Standardeinstellungen gezeigt, welche auch ein „zuviel“ an Datenverarbeitung beinhalten, und ein sehr einfacher Weg, weitere Detaileinstellungen „abzukürzen“, das heißt alles wie eingestellt zu akzeptieren. Der Aufwand, jede Einstellung tatsächlich zu beeinflussen, ist ungleich länger und komplexer gestaltet (daher auch eine Behinderungstaktik).
- Einbau von Widersprüchen, wie zum Beispiel das Versprechen, jederzeit Sichtbarkeitseinstellungen vornehmen zu können, dann aber relativieren, dass bei bereits sichtbaren Posts irgendetwas Negatives passieren kann.
- Falschinformationen, zum Beispiel „wie eine Einwilligung widerrufen werden kann“: Ein Element der Oberfläche ist so designt, dass dort nicht die (erwartete) Funktion des Widerspruchs eingeblendet wird, sondern nur allgemeine Informationen, was ein Widerspruch ist und auf welchem Recht das beruht. Der eigentliche Weg des Widerspruchs bleibt versteckt.

- Informationspräsentation schlecht strukturiert (zu komplex, zu einfach):
    - Zu komplex: In der Dokumentation sind zu viele Verweise an zu vielen Stellen und wesentliche Informationen werden erst in unteren Ebenen bereitstellt.
    - Zu einfach: Datenschutzerklärung ist unstrukturierter Textblock, der sich über viele Seiten zieht und keine sinnvollen Navigationspunkte wie Teilüberschriften oder Themenkomplexe enthält.
- Verwendung unklarer Begriffe: Es wird auf Begriffe verwiesen, welche unklar oder mehrdeutig sind, um so bewusst Interpretationsspielraum zu schaffen (Beispiele sind „Verbesserung von Produkten“, „Nutzeraktivitäten“, „Bereitstellung eines Dienstes“) und den Nutzer im Unklaren lassen, welche konkreten personenbezogenen Daten zu welchen konkreten Verarbeitungszwecken genutzt werden. Es werden Begriffe erfunden, welche nur unter großer Mühe irgendwo im Text einer Bedeutung zugeordnet werden können (zum Beispiel „erzeugte Daten“, wobei erst auf Seite 80 steht, „erzeugte Daten können auch personenbezogene Daten enthalten“).
- Einwilligungsoptionen auf unklare Begriffe: Ein Nutzer ist sich nicht im Klaren, was zum Beispiel Einwilligung in die Verarbeitungszwecke „Datenschutz“, „Sicherheit“, „Inhalte“, „Privatsphäre“ oder „Deine Einstellungen“ bedeutet und kann daher nicht informiert entscheiden.
- Sprachbrüche: Einzelne Teile der Information liegen in der Sprache des Zielmarktes vor (wie zum Beispiel zur Abrechnung, zu den Möglichkeiten der Plattform), aber andere Teile der notwendigen Informationen sind nur zum Beispiel in englischer Sprache vorhanden.
- Verwirrendes Interface: Informationen sind nur umständlich zu finden und durch schlecht zu bedienende grafische Elemente erreichbar (zum Beispiel Suchmaske in eine große, beliebig strukturierte Menge an Dokumenten ohne weitere Navigationsfunktion oder Hilfe).
- Ungültige Links: Wichtige Informationen werden per Link eingebunden, welcher aber nicht funktioniert.
- Einstellelemente (Schalter) sind so designt, dass unklar ist, wann der Schalter auf „Ein“ steht und wann auf „Aus“.

- Unklares Verhalten der Oberfläche: Wenn Nutzer Einstellungen auf der Nutzeroberfläche ändern, passiert gar nichts und der Nutzer wird im Unklaren gelassen, ob die neuen Einstellungen wirklich erkannt und akzeptiert wurden.
- Einstellungen außerhalb des Kontexts: Einstellungen (zum Beispiel zur Einwilligung) sind in Teilen der Oberfläche versteckt, an welchen andere Themen steuerbar sind und diese Einstellungen nicht vermutet werden können.

Alle diese Punkte weisen zumindest auf ein schlechtes Design der App oder Webseite des sozialen Netzwerks hin. Sie führen nicht in jedem Fall dazu, dass das soziale Netzwerk rechtlich unzulässig wäre, sind aber zumindest deutliche Indizien für einen möglichen Verstoß. Solche Verstöße können im Einzelfall darin zu sehen sein, dass eine an sich notwendige Einwilligung der Nutzer in die Datenverarbeitung nicht eingeholt wird und die Datenverarbeitung damit unzulässig ist, sofern neben der Einwilligung keine andere Rechtsgrundlage in Betracht kommt. Daher sollten Bürger bei der Auswahl von sozialen Netzwerken durchaus darauf achten, ob solche problematischen Verhaltensweisen der Anwendung erkennbar sind, da diese auch eine Aussage darüber treffen könnten, wie ernst das jeweilige soziale Netzwerk das Thema Datenschutz wirklich nimmt.
Dem Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit sind diese Festlegungen bei seinen Beratungen sehr hilfreich und er wird sie auch bei seinen Prüfungen zugrundelegen.
Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hatte bereits wichtige Aspekte dieser Leitlinien in ihre „*Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) Version 1.1*“ einfließen lassen (https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf).

1.19 Stand Umsetzung § 10 Elektronischer-Rechtsverkehr-Verordnung

Die Umsetzung des „besonderen elektronische Bürger- und Organisationspostfaches“ verzögert sich weiter. Ursprünglich zum zweiten Quartal 2022 geplant, ist jetzt der nächste Termin frühestens im zweiten Quartal 2023 vorgesehen.

Bereits 2017 veröffentlichte die Bundesregierung die „Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach – Elektronischer Rechtsverkehr Verordnung“ (kurz ERVV), welche unter anderem die sichere elektronische Kommunikation Dritter mit den Gerichten regelt. 2021 wurde die Verordnung so erweitert, dass nun auch Bürger und Organisationen (wie Vereine, Wirtschaftsunternehmen) teilnehmen können sollen. Der § 10 ERVV regelt dazu die Voraussetzungen des besonderen elektronischen Bürger- und Organisationspostfaches.
Im letzten Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde unter Punkt 1.15 (Seite 62 ff) bereits berichtet, dass neben dem besonderen elektronische Behördenpostfach (beBPo), dem besonderen elektronischen Notarpostfach (beN) und dem besonderen elektronischen Anwaltspostfach (beA) auch ein kostenfreies Nutzerkonto für Bürger und Organisationen (eBO) für die sichere Kommunikation mit der Justiz geplant ist. Der Funktionsumfang der Nutzerkonten wurde hierfür erweitert und sollte nach damaligen Planungen voraussichtlich im zweiten Quartal 2022 zur Verfügung stehen.
Der Webseite https://egvp.justiz.de/buerger_organisationen/index.php ist nun zu entnehmen, dass dieses kostenfreie Postfach für Bürger und Organisationen voraussichtlich erst im zweiten Quartal 2023 zur Verfügung stehen soll.
Somit müssen Bürger und Organisationen weiterhin warten, um Dokumente rechtssicher auch auf elektronischem Wege an die Gerichte über dieses Verfahren übermitteln zu können. Der TLfDI wird über den weiteren Verlauf berichten.

1.20 BSI-Veröffentlichungen 2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig dem aktuellen Stand der Technik entsprechende Hinweise, Richtlinien und Mindeststandards. Der TLfDI empfiehlt, eigene Daten, Systeme und Informationen dahingehend zu überprüfen, ob sie den aktuellen Empfehlungen des jeweiligen IT-Grundschutz-Kompendiums entsprechen oder Handlungsbedarf in technischer oder/und organisatorischer Hinsicht besteht.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig dem aktuellen Stand der Technik entsprechende Hinweise, Richtlinien und Mindeststandards. Drei der 2022 veröffentlichten Dokumente rückt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in den Blickpunkt:

IT-Grundschutz-Kompendium (Edition 2022)

Mit dem IT-Grundschutz-Kompendium bietet das BSI ein Werkzeug an, wie die Informationssicherheit einer Institution angemessen geschützt werden kann. Das IT-Grundschutz-Kompendium des BSI wird jährlich im Februar in einer neuen Edition veröffentlicht. Die Edition 2022 enthält 104 IT-Grundschutz-Bausteine, wobei davon in der aktuellen Edition 16 überarbeitet wurden. So sind zum Beispiel die Bausteine Datensicherungskonzept, Protokollierung, Fernwartung und Clients unter Windows 10 dem aktuellen Stand der Technik angepasst worden.

Der TLfDI empfiehlt, regelmäßig eigene Systeme dahingehend zu überprüfen, ob sie den aktuellen Maßgaben des IT-Grundschutz-Kompendiums entsprechen oder Handlungsbedarf in technischer oder/und organisatorischer Hinsicht besteht: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=5

Anforderungen an Anwendungen im Gesundheitswesen (BSI TR-03161)

Das BSI hat die Technische Richtlinie (TR) „Anforderungen an Anwendungen im Gesundheitswesen“ aktualisiert. Diese TR richtet sich an Hersteller von Anwendungen im Gesundheitswesen. Sie gliedert sich in drei Teile.

Teil 1: Die TR Mobile Anwendungen (BSI TR-03161-1) liegt nun mit Stand Juni 2022 in der Version 2.0 vor. Wesentliche Änderungen ergeben sich aus der Erstellung der Prüfschritte (Kapitel 4) und der Erstellung der Risikoanalyse (Kapitel 5). So sind in den Prüfschritten beispielsweise zu untersuchen, welchen Zweck die Verarbeitung von personenbezogenen Daten hat, ob auch ohne Zustimmung des Nutzers personenbezogene Daten verarbeitet werden können und ob beziehungsweise wie die Datenübermittlung an Dritte geregelt ist. Auch die Aspekte der Speicherung und der Zugriff auf besondere personenbezogene Daten gemäß Art. 9 DS-GVO sind gemäß den Schritten zu prüfen.

Teil 2: Web-Anwendungen (BSI TR-03161-2) ist neu und liegt mit Stand Juni 2022 in der Version 1.0 vor. Dieser Teil richtet sich an Hersteller von Web-Anwendungen im Gesundheitswesen. Aus der Sicht des BSI kann sie zusätzlich auch als Richtlinie für Web-Anwendungen betrachtet werden, die besondere Kategorien von personenbezogenen Daten verarbeiten.
Teil 3: Hintergrundsysteme (BSI TR-03161-3) ist ebenfalls neu und liegt mit Stand Juni 2022 in der Version 1.0 vor. Dieser Teil der Technischen Richtlinie (TR) richtet sich an Hersteller von Hintergrundsystemen für Anwendungen im Gesundheitswesen. Zusätzlich kann auch dieser Teil als Richtlinie für Hintergrundsysteme betrachtet werden, welche besondere personenbezogene Daten verarbeiten. Hintergrundsysteme speichern in diesem Fall sensible und persönliche Daten, von der Pulsfrequenz, über Aufzeichnungen des Schlafrhythmus bis hin zu Medikationsplänen sowie ärztlichen Verordnungen und Bescheinigungen. Sie verbinden den Nutzer und dessen personenbezogene Daten mit entsprechenden Services und fungieren als Kommunikations-Knotenpunkte. Eine kompromittierte Anwendung und deren Hintergrundsystem kann so das gesamte digitale Leben des Nutzers ungewollt offenlegen und zu hohem persönlichen und auch finanziellen Schaden führen. Das Einhalten von geeigneten Sicherheitsstandards, gerade im Bereich der Hintergrundsysteme, kann dieses Kompromittieren wesentlich erschweren und sogar verhindern. Schon während der Entwicklungsphase einer Anwendung sollten Hersteller deshalb sehr verantwortungsvoll planen, wie ein Hintergrundsystem personenbezogene Daten und besondere Kategorien von personenbezogenen Daten verarbeitet und gegen Missbrauch schützt.
Die Richtlinie mit den drei Teilen ist abrufbar unter: BSI TR-03161 Sicherheitsanforderungen an digitale Gesundheitsanwendungen (bund.de).

Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (zum Beispiel Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden (BSI TR-03170)
Das BSI hat die Technische Richtlinie (TR) „Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (zum Beispiel Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden mit Veröffentlichung der Version 6.0 aktualisiert. Sie regelt die digitale Übermittlung biometrischer Lichtbilder von Dienst-

leistern (zum Beispiel Fotografinnen und Fotografen) an Pass-, Personalausweis- oder Ausländerbehörden über einen sicheren Cloud-Dienst und definiert Anforderungen für die Zertifizierung von Diensten für dieses spezielle Verfahren. Laut Richtlinie wird allen zuständigen Behörden hierbei der Abruf der Lichtbilder von so zertifizierten Dienstanbietern ermöglicht. Die Richtlinie mit den drei Teilen „Grundlegende Rahmenbedingungen“, „Anforderungen an den Cloud-Dienst“, „Anforderungen an die Software“ ist in der Version 0.6 abrufbar unter: BSI TR-03170 (bund.de).

2. Fälle öffentlicher Bereich

Rathaus Architektur Gebäude - Kostenloses Bild auf Pixabay

2.1 Polizeirecherche – ohne Grenzen?

Mit einer namensbasierten Rufnummeranfrage nach Art. 173 Abs. 4 Nr. 1 Telekommunikationsgesetz (TKG) verstieß eine Polizeiinspektion gegen datenschutzrechtliche Bestimmungen. Diese Feststellung des TLfDI stützte sich darauf, dass im vorliegenden Fall offensichtlich gegen den im Grundgesetz – in Artikel 20 Abs. 3 GG – verankerten Grundsatz der Verhältnismäßigkeit verstoßen wurde.

Im Rahmen einer Beschwerde erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis darüber, dass eine Thüringer Polizeiinspektion entgegen datenschutzrechtlicher Bestimmungen die Handynummer eines Beschwerdeführers recherchiert hatte. Zum Hintergrund des Vorfalls kann gesagt werden, dass der Beschwerdeführer Zeuge im Rahmen einer Unfallfluchtermittlung war, dabei jedoch lediglich seine Postadresse sowie seine damalige „alte“ Handynummer angegeben hatte. Groß war für den Beschwerdeführer daher die Verwunderung, als er durch die für das Verfahren zuständige Polizeidienststelle telefonisch unter seiner „neuen“ Handynummer kontaktiert wurde. Auf Nachfrage des Beschwerdeführers teilte ihm die Polizeiinspektion im Rahmen des Telefonates lapidar mit, dass die Telefonnummer recherchiert

worden sei. Außerdem teilte die Polizeiinspektion dem Beschwerdeführer mit, dass sie ihre Nachfrage an ihn als Zeugen auch schriftlich hätte stellen können.
Nachdem der TLfDI die zuständige Polizeiinspektion um Stellungnahme ersucht hatte, erhielt er von der vorgesetzten Landespolizeiinspektion die Rückmeldung, dass im vorliegenden Fall eine nach § 173 Abs. 4 Nr. 1 Telekommunikationsgesetz (TKG) namensbasierte Rufnummeranfrage bei der Bundesnetzagentur gestellt worden war. Nach § 173 Abs. 4 Nr. 1 TKG erteilt die Bundesnetzagentur den Strafverfolgungsbehörden Auskünfte aus den Kundendateien, soweit unter anderem die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Als Rechtfertigung hierfür wurde durch die Landespolizeiinspektion angegeben, dass die vom Beschwerdeführer angegebene Rufnummer ungültig war. Da der Beschwerdeführer schon einmal eine Rufnummer angegeben hätte, sei davon auszugehen, dass er damit einverstanden sei, fernmündlich kontaktiert zu werden, so die Aussage der Polizeiinspektion.
Der TLfDI war nach Prüfung des zugrundeliegenden Sachverhalts zu dem Ergebnis gelangt, dass durch die streitgegenständliche namensbasierte Rufnummeranfrage nach § 173 Abs. 4 Nr. 1 TKG ein Verstoß gegen datenschutzrechtliche Bestimmungen gegeben war. Diese Feststellung stützte sich darauf, dass im vorliegenden Fall offensichtlich gegen den im Grundgesetz (GG) – in Art. 20 Abs. 3 GG – verankerten Grundsatz der Verhältnismäßigkeit verstoßen wurde. Der Grundsatz der Verhältnismäßigkeit verlangt als Grundsatz des öffentlichen Rechts und des Strafrechts, dass jedes staatliche Handeln in Hinblick auf den verfolgten Zweck geeignet, erforderlich und angemessen sein muss (vergleiche dazu Sachs in: Sachs, Grundgesetz-Kommentar, 7. Auflage, Art. 20, Rn. 149 ff.).
Zunächst war die namensbasierte Rufnummeranfrage geeignet, den angestrebten Zweck zu erreichen. Die Kontaktaufnahme durch die Polizeiinspektion mit dem Zeugen konnte – nach Auffassung der Polizeiinspektion – erfolgreich durchgeführt werden.
Für eine ordnungsgemäße Ausübung des behördlichen Auswahlermessens ist es allerdings im Rahmen der polizeilichen Ermittlungen auch zwingend notwendig, dass nach dem Begriff der Erforderlichkeit gemäß § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) das zur Erreichung des Erfolges mildeste Mittel gleicher Wirksamkeit eingesetzt werden muss (vergleiche auch so Sachs, a.a.O., Art. 20, Rn. 152).

Für den hier zugrundeliegenden Fall bedeutete dies, dass erst dann eine namensbasierte Rufnummeranfrage hätte durchgeführt werden dürfen, wenn andere, weniger in das Grundrecht auf informationelle Selbstbestimmung eingreifende Maßnahmen zur Kontaktaufnahme mit dem Beschwerdeführer als Zeugen, die eine geringere Eingriffsintensität in seine Persönlichkeitsrechte haben, nachweislich erfolglos ergriffen worden waren.
Eine mildere Maßnahme zur Kontaktaufnahme wäre vorliegend eine schriftliche Nachfrage durch die Polizeiinspektion beim Beschwerdeführer gewesen. In diesem Zusammenhang wäre es sowohl möglich gewesen, etwaige Unklarheiten im Rahmen der Zeugenvernehmung des Beschwerdeführers zu klären als auch eine aktuelle telefonische Erreichbarkeit bei dem Beschwerdeführer abzufragen.
Der Schlussfolgerung der Polizeiinspektion, dass davon ausgegangen werden konnte, dass der Beschwerdeführer mit der fernmündlichen Kontaktaufnahme einverstanden war, weil er bereits einmal seine Rufnummer angegeben hatte, konnte der TLfDI in diesem Zusammenhang nicht folgen. Dies war nämlich keine Rechtfertigung beziehungsweise keine nur annähernd ausreichende Begründung für den weitreichenden Eingriff in die Persönlichkeitsrechte des Betroffenen in Form einer namensbasierten Rufnummeranfrage. Dementsprechend räumte die Polizeibeamtin, die den telefonischen Kontakt mit dem Beschwerdeführer aufgenommen hatte, im Rahmen der Anhörung gegenüber dem TLfDI ein, dass diese Kontaktaufnahme auch schriftlich hätte erfolgen können.
Weitere Gründe, weshalb eine fernmündliche der schriftlichen Kontaktaufnahme vorgezogen wurde beziehungsweise die diese gegebenenfalls rechtfertigen würden, wurden durch die Polizeiinspektion offengelassen.
Im Ergebnis stellte der TLfDI deshalb fest, dass unter Beachtung des Verhältnismäßigkeitsgrundsatzes gemäß Art. 20 Abs. 3 GG keine namensbasierte Rufnummeranfrage zum Beschwerdeführer nach § 173 Abs. 4 Nr. 1 TKG erforderlich gewesen ist. Die namensbasierte Rufnummeranfrage hat somit den Beschwerdeführer in seinem verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung verletzt.
Da die personenbezogenen Daten des Beschwerdeführers im Rahmen einer Unfallfluchtermittlung verarbeitet worden sind, handelte es sich vorliegend um keinen datenschutzrechtlichen Verstoß, der unter den Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO)

fällt. Vielmehr fiel dieser Datenschutzverstoß in den Anwendungsbereich der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (sogenannte JI-Richtlinie), die mit den §§ 31 ff. ThürDSG in Landesrecht umgesetzt worden ist. Um den datenschutzrechtlichen Verstoß, hier vorliegend die namensbasierte Rufnummeranfrage, zu sanktionieren, beanstandete der TLfDI das Vorgehen der Polizeiinspektion gemäß § 7 Abs. 6 Satz 1 ThürDSG, da die zuständige Polizeiinspektion als ersuchende Behörde die Verantwortung für die namensbasierte Rufnummeranfrage trägt (vergleiche § 173 Abs. 7 Nr. 2 TKÜ).
Als Konsequenz der vom TLfDI ausgesprochenen Beanstandung sensibilisierte die zuständige Polizeiinspektion nicht nur die betroffene Polizeibeamtin, sondern alle Kolleginnen und Kollegen des zuständigen Polizeiermittlungsdienstes hinsichtlich der Einhaltung der Voraussetzungen für die Anwendung einer nach § 173 Abs. 4 Nr. 1 TKG namensbasierten Rufnummeranfrage. Zusätzlich wurden beziehungsweise werden innerhalb der Thüringer Polizei entsprechende Schulungen im Rahmen der Aus- und Fortbildung initiiert.

2.2 Die Nutzung von WhatsApp und eines privaten E-Mail-Kontos im Ordnungswidrigkeitenverfahren

Die unbedarfte Nutzung privater Endgeräte für die Verarbeitung personenbezogener Daten im Rahmen der dienstlichen Arbeit kann, wie im vorliegenden Fall, einen datenschutzrechtlichen Verstoß begründen. Der TLfDI gelangte in diesem Fall zu dem Ergebnis, dass durch die Anfertigung und die dreifache Übermittlung eines Fotos von einem Fahrzeug mit dem sichtbaren amtlichen Kennzeichen via WhatsApp ein Verstoß gegen die Anforderungen, die sich aus dem Grundsatz der Vertraulichkeit im Zusammenhang mit der Verarbeitung gemäß § 54 Abs. 1 Satz 1, Abs. 2 Satz 2. Nr. 1 ThürDSG ergeben, vorlag.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde gegen eine Stadt in Thüringen. Darin teilte der Beschwerdeführer mit, dass er eine Verwarnung mit Verwarnungsgeld von der Stadt erhalten habe. Hintergrund war, dass er nicht am rechten Fahrbahnrand parkte und daher eine Ordnungswidrigkeit im Raum stand. Als Beweismittel diente ein Foto. Dieses hatte die Dateibezeichnung mit der Endung „0004.ipg“.

Nach Auffassung des Beschwerdeführers war die Endung „0004“ ein Hinweis darauf, dass dieses Foto bereits vorher dreimal in Verwendung war oder als viertes Foto im Ordnungsamt gespeichert wurde. Des Weiteren führte der Beschwerdeführer in seiner Beschwerde aus, dass die Beweisfotos wohl mit Android-Handys aufgenommen und via WhatsApp an das Ordnungsamt geschickt worden seien. Er ging davon aus, dass weitere personenbezogene Daten wie sein Name und seine Adresse in die Hände des Bediensteten, der das Foto fertigte, gelangten und weiterverbreitet wurden.
Die nachfolgende Sachverhaltsermittlung des TLfDI nahm leider eine sehr lange Zeit in Anspruch. Der TLfDI musste mit der verantwortlichen öffentlichen Stelle einen regen Schriftverkehr führen, um den Sachverhalt schlussendlich zu ermitteln. Dieses Verhalten der Stadt beanstandete der TLfDI im Nachgang auch gemäß § 7 Abs. 6 Satz 1 Thüringer Datenschutzgesetz (ThürDSG), weil die Stadt als Verantwortliche die Fragen des TLfDI zur Aufklärung des Sachverhalts einfach nicht beantwortete und zugleich die datenschutzrechtliche Prüfung der Übermittlung des streitgegenständlichen Fotos durch verfahrensverschleppende Verzögerungen behinderte.
Eine Beanstandung als Maßnahme des TLfDI kommt immer dann zur Anwendung, wenn Verstöße gegen die Vorschriften des Datenschutzes bei der Verarbeitung von personenbezogenen Daten vorliegen, die nicht im Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) erfolgt. Da die Stadt personenbezogene Daten im Rahmen eines Ordnungswidrigkeitenverfahrens verarbeitete, kam in diesem Fall nicht die DS-GVO zur Anwendung, sondern die JI-Richtlinie 2016/680, die im ThürDSG beziehungsweise im Bundesdatenschutzgesetz umgesetzt ist.
Neben der zähen Sachverhaltsaufklärung stand natürlich auch der vorgetragene Datenschutzverstoß im Fokus. Der Sachverhalt stellte sich so dar, dass ein Bediensteter der Stadt das Foto vom Fahrzeug des Beschwerdeführers mit seinem privaten Handy aufnahm und es via WhatsApp an eine weitere Mitarbeiterin der Stadt sendete. Diese wiederum schickte sich das Foto auf ihre private E-Mail-Adresse und von dort aus an die dienstliche E-Mail-Adresse. Daraufhin wurde ein Ordnungswidrigkeitenverfahren gegen den Beschwerdeführer von Seiten der Stadt eingeleitet.
Dieser Sachverhalt beinhaltete mehrere Verletzungen gegen datenschutzrechtliche Vorschriften:

Gemäß § 31 ThürDSG galten für diesen Fall die Bestimmungen des 3. Abschnitts des ThürDSG für die Verarbeitung personenbezogener Daten durch die für die Verfolgung von Ordnungswidrigkeiten zuständige öffentliche Stelle, da die Daten zum Zweck der Erfüllung dieser Aufgaben verarbeitet wurden. Die Stadt war dabei als Verantwortliche anzusehen. Ausweislich der Einlassungen der Stadt fertigte einer ihrer Bediensteten mit seinem sonst ausschließlich für private Zwecke genutzten Mobilfunkgerät (= Handy) von dem Fahrzeug des Beschwerdeführers ein Foto. Dieses diente als Beweis im sodann gegen den Beschwerdeführer eingeleiteten Ordnungswidrigkeitenverfahren. Das Foto ließ das amtliche Kennzeichen des Fahrzeugs deutlich erkennen. Amtliche Kennzeichen stellen personenbezogene Daten dar. Gemäß § 32 Nr. 1 ThürDSG sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Der Beschwerdeführer konnte anhand des amtlichen Kennzeichens über die Auskunft beim Kraftfahrtbundesamt identifiziert werden. Damit erhob der Bedienstete der Stadt im vorliegenden Fall ein personenbezogenes Datum.
Das Erheben personenbezogener Daten stellt wiederrum eine Verarbeitung im Sinne des § 32 Nr. 2 ThürDSG dar.
Die Stadt war Verantwortliche im Sinne des § 32 Nr. 7 ThürDSG. Danach ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Bedienstete der Stadt hatte die Anzeige in seiner dienstlichen Funktion als Mitarbeiter der Stadtmeisterei erstattet, da er aufgrund des durch den Beschwerdeführer ordnungswidrig abgestellten Fahrzeuges seinem dienstlichen Mähauftrag nicht vollumfänglich habe nachkommen können. In diesem Rahmen entschied er als Bediensteter der Stadt über Zwecke und Mittel der Verarbeitung des personenbezogenen Datums des Beschwerdeführers in Form des amtlichen Kfz-Kennzeichens. Hieran änderte auch das vorgebrachte Argument nichts, dass eine Vereinbarung zur Nutzung

privater Endgeräte für dienstliche Zwecke nicht bestanden habe und die praktizierte Verfahrensweise auf eigene Initiative ohne dienstliche Weisung des Bediensteten erfolgte und eine entsprechende dienstrechtliche Weisung zu keiner Zeit bestand. Die Stadt führte nämlich im Rahmen der Verwarnung an den Beschwerdeführer das Beweismittel „Foto, Zeuge“ auf. Ihr war bekannt, dass der Bedienstete im Rahmen seiner dienstlichen Tätigkeit unter der Adresse der Stadtmeisterei die Anzeige erstattete, und sie verwendete ferner auch seine Zeugenaussage als Beweismittel. Damit musste sie sich auch die Verantwortlichkeit für die Datenverarbeitung anrechnen lassen. Im Übrigen waren keinerlei Hinweise erkennbar, dass der Bedienstete der Stadt das Foto aus privaten Gründen aufgenommen hätte. Die Stadt war somit im Ordnungswidrigkeitenverfahren gemäß § 31 Satz 2 ThürDSG die datenschutzrechtlich verantwortliche Stelle.

Gemäß § 54 Abs. 1 Satz 1 ThürDSG hat der Verantwortliche unter Berücksichtigung des Standes der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Gemäß § 54 Abs. 2 Satz 2 Nr. 1 ThürDSG sollen die Maßnahmen nach Absatz 1 dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden. § 54 Abs. 2 Satz 2 Nr. 1 ThürDSG entspricht dabei Art. 32 Abs. 1 Buchstabe b) DS-GVO. Weder das ThürDSG noch die DS-GVO definieren den Begriff „Vertraulichkeit“. Es kann jedoch auf die Definition aus der Informationssicherheit zurückgegriffen werden (so Hansen in Simitis/Hornung/Spiecker, 1. Auflage 2019, Art. 32 Rdn. 39): „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ (vergleiche Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundschutz-Kompendium Edition 2022).

Die Erhebung eines personenbezogenen Datums zu dienstlichen Zwecken mit einem sonst ausschließlich privat genutzten Mobilfunkgerät

stellte im hier zu entscheidenden Fall einen Verstoß gegen die Vertraulichkeit gemäß § 54 Abs. 2 Satz 2 Nr. 1 ThürDSG dar. Der Schutz vor unbefugter Preisgabe von Informationen war nicht gewährleistet oder durch die Dienststelle überprüfbar. Insbesondere war nicht auszuschließen, dass unbefugte dritte (Privat-)Personen Zugriff auf das Gerät haben konnten oder die aufgenommenen Fotos durch Dienste auf dem Smartphone an Drittdienste übermittelt worden wären. Fast immer findet ein Datenaustausch mit den Softwareherstellern und eine cloudbasierte Sicherung von Fotos statt, sodass darüber ein Zugriff Dritter (zum Beispiel des Softwareherstellers) möglich ist. Hinzukommt, dass die Softwarehersteller ihren Sitz in Drittländern außerhalb der EU haben, wie beispielweise den USA, und aufgrund der dortigen Gesetzeslage ein Zugriff unbefugter Dritter nicht ausgeschlossen werden kann.

Doch selbst wenn ein Zugriff Dritter auf das Foto auf dem privaten Mobilfunkgerät des Bediensteten hätte ausgeschlossen werden können, lag ein Verstoß gegen die Vertraulichkeit vor, und zwar in Form der Übermittlung des Fotos mittels Privathandy mit dem Messenger-Dienst WhatsApp. Die Datenverarbeitung erfolgte nicht in einer Weise, die ein dem Risiko angemessenes Schutzniveau sicherstellte. Insbesondere war der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust nicht durch geeignete technische und organisatorische Maßnahmen gewährleistet.

WhatsApp gehört zur Meta Platforms Inc. (vorher Facebook), welche in den USA ansässig ist. Fotos werden bei WhatsApp kurzzeitig zwischengespeichert. Zudem können Chatverläufe auf Google Drive oder Apple iCloud gesichert werden. Hierbei entfällt bei der Nutzung von Google Drive die Ende-zu-Ende-Verschlüsselung, sodass unverschlüsselte Daten bei dem ebenfalls US-amerikanischen Cloudanbieter liegen. Die Verarbeitungszwecke, zu welchen die Fotos durch Drittdienste verarbeitet werden, unterliegen den Nutzungsverträgen der jeweiligen Privatnutzer und können über die für die Anzeige notwendigen Verarbeitungszwecke hinausgehen. Dies schließt eine Offenlegung der Inhalte gegenüber Dritten gegebenenfalls mit ein und ist vom jeweiligen Dienst abhängig. Gemäß der Entscheidung des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer, Az. C-311/18 (Schrems II), bietet das US-Recht, wie beispielweise die nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12 333, kein ausreichendes Schutzniveau, mit welchem ein Zugriff Dritter (zum Beispiel der

Nachrichtendienste) ausgeschlossen ist. Es war also nicht sichergestellt, dass das im vorliegenden Fall gefertigte Beweisfoto Dritten unzugänglich war. Damit war es nicht ausschließlich Befugten in der zulässigen Weise zugänglich.
Auch hinsichtlich der Übermittlungen des als Beweis gefertigten Fotos vom Fahrzeug des Beschwerdeführers durch eine weitere Bedienstete von ihrem privaten Mobilfunkgerät an ihre private E-Mail-Adresse und von dort an ihre dienstliche E-Mail-Adresse war die Stadt Verantwortliche gemäß § 32 Nr. 7 ThürDSG. Sie entschied über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten, weil die Bedienstete die Übermittlungen im Rahmen ihrer dienstlichen Tätigkeit als Sachbearbeiterin des Amtes für Sicherheit und Ordnung bei der Stadt vornahm. Sie eröffnete im Nachgang ein Ordnungswidrigkeitenverfahren gegen den Beschwerdeführer. Es bestanden keinerlei Anhaltspunkte, dass sie Veranlassung gehabt hätte, die Übermittlungen als Privatperson vorzunehmen. Damit musste sich die Stadt die Verantwortlichkeit zurechnen lassen.
Die Übermittlung des gefertigten Fotos vom Fahrzeug des Beschwerdeführers inklusive des amtlichen Kennzeichens von dem privaten WhatsApp-Account der Bediensteten an ihre private E-Mail-Adresse sowie die Übermittlung von dort aus an die dienstliche Outlook-E-Mail-Adresse stellte einen Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit im Zusammenhang mit der Verarbeitung gemäß § 54 Abs. 1 Satz 1, Abs. 2 Satz 2 Nr. 1 ThürDSG dar.
Der Schutz vor unbefugter Preisgabe von Informationen war durch die Übermittlung von einem privaten WhatsApp-Account der Bediensteten an ihre private E-Mail-Adresse nicht gewährleistet. Insbesondere war nicht auszuschließen, dass unbefugte dritte (Privat-)Personen Zugriff auf ihre private E-Mail-Adresse hätten haben können. Zu nennen wäre hier insbesondere der beteiligte E-Mail-Provider, welcher durch die gewählte Übertragung Einsicht in den Inhalt der besagten E-Mails erhalten kann. Da keine Anhaltspunkte bezüglich der genutzten Verschlüsselung der E-Mail genannt wurden, welche das Foto transportierte, musste der TLfDI davon ausgehen, dass das Foto sowohl auf dem Smartphone der Bediensteten als auch bei dem E-Mail-Provider im Klartext einsehbar war. Insbesondere die Verarbeitungszwecke des E-Mail-Providers beinhalteten auch Datenübermittlungen an Drittdienstleister zur „Datenanalyse“, welche nicht dienstlich erforderlich waren und die Vertraulichkeit der E-Mail-Inhalte gefährden konnten.

Ferner konnte nicht vom Vorliegen der notwendigen technisch-organisatorischen Voraussetzungen zur Absicherung personenbezogener Daten, insbesondere auch auf dem Transportweg zwischen WhatsApp und dem privaten E-Mail-Account, ausgegangen werden.
Bei privaten E-Mail-Adressen hängt das technische Schutzniveau weithin von der willkürlichen Konfiguration der Nutzer und der Konfiguration der E-Mail-Provider ab – ein Prüfmechanismus analog § 48 Abs. 6 Nr. 5 ThürDSG liegt hier nicht vor. Der Schutz vor Fremdzugriffen kann nicht sichergestellt werden. Zum Schutz der Vertraulichkeit der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der Technischen Richtlinie 03108-1 des Bundesamts für Sicherheit in der Informationstechnik einhalten. Dies ist aber beim Versand an nichtdienstliche Adressen nicht sichergestellt.
Verantwortliche, die öffentliche E-Mail-Diensteanbieter als Empfänger ihrer Nachrichten in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen des ThürDSG und insbesondere der genannten Technischen Richtlinie bieten.
Aus diesem Grund beanstandete der TLfDI gemäß § 7 Abs. 6 ThürDSG zum einen, dass der Bedienstete der Stadt das Foto mit seinem privaten Mobilfunkgerät fertigte und über den Messenger-Dienst WhatsApp an die privaten Kontaktdaten der anderen Bediensteten übermittelte. Zum anderen beanstandete der TLfDI, dass die andere Bedienstete der Stadt das Foto des Beschwerdeführers inklusive des amtlichen Kennzeichens von ihrem privaten Mobilfunkgerät aus dem Messenger WhatsApp an ihre private E-Mail-Adresse und von dort an ihr dienstliches E-Mail-Postfach übermittelte.
Die Stadt reichte Klage gegen die Beanstandung des TLfDI ein. Das Gerichtsverfahren war im Berichtszeitraum noch nicht abgeschlossen. Der TLfDI wird im nächsten Tätigkeitsbericht über den Ausgang des Verfahrens berichten.

2.3 Eine Frage der Eh(r)e

Jede Person kann sich mit einer Beschwerde über eine mögliche Datenschutzverletzung an den TLfDI wenden. Ein Anspruch auf die Durchsetzung einer bestimmten aufsichtsrechtlichen Maßnahme gemäß Art 58 Abs. 2 DS-GVO (Verwarnung, Anweisung, Beschränkung etc.) besteht aber grundsätzlich nur im Falle einer (möglichen)

Verletzung von eigenen Rechten sowie (kumulativ) einer Reduktion des Ermessens auf Null (das heißt, nur eine einzelne Maßnahme in einer konkreten Situation wäre rechtmäßig). Daher besteht regelmäßig nur ein subjektiv-öffentliches Recht auf fehlerfreie Ermessensausübung der Aufsichtsbehörde (siehe dazu VG Ansbach, Urteil vom 8. August 2019, Aktenzeichen AN 14 K 19.00272, Rn. 43 der juris-Entscheidung; ähnlich VG Wiesbaden, Urteil vom 24. September 2021, Aktenzeichen 6 K 442/21.WI, Rn. 33 der juris-Entscheidung; im Ergebnis auch VGH Baden-Württemberg, Urteil vom 22. Januar 2020, Aktenzeichen 1 S 3001/19, Rn. 51 der juris-Entscheidung).

Ein Ehepaar – die Beschwerdeführerin und der Beschwerdeführer – wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und trug eine Datenschutzbeschwerde vor. Bei einem Gespräch in der Ausländerbehörde habe die Beschwerdeführerin den Verdacht geäußert, dass eine ihr bekannte Person (im Weiteren wird diese Person zur besseren Verständlichkeit Herr X genannt) eine Scheinehe führe. Im Nachgang zu diesem Gespräch habe dann ihr Mann erfahren, dass Herr X von der städtischen Ausländerbehörde wohl die Auskunft erhalten habe, dass der Beschwerdeführer den Verdacht einer möglicherweise geführten Scheinehe geäußert habe. Dabei soll die Mitarbeiterin der Ausländerbehörde Herrn X auch noch eine Kopie des Personalausweises des Beschwerdeführers vorgelegt haben.
Zur Aufklärung und Prüfung des vorgetragenen Beschwerdesachverhalts übte der TLfDI sein Entschließungsermessen zum Tätigwerden auf der Grundlage von Art. 57 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) und Art. 58 Abs. 1 Buchstabe b) DS-GVO in Verbindung mit § 6 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sowie § 28 Thüringer Verwaltungsverfahrensgesetz aus, wandte sich an die Stadt und ersuchte diese um eine Stellungnahme. Nachdem die Stadt mitteilte, dass sie weder den Beschwerdeführer als Hinweisgeber für eine mögliche Scheinehe des Herrn X diesem gegenüber benannt noch Herrn X eine Ausweiskopie des Beschwerdeführers gezeigt hätte, musste der TLfDI feststellen, dass in dem von ihm datenschutzrechtlich zu beurteilenden Sachverhalt zwei sich widersprechende Darstellungen vorlagen. Dies hatte wiederum zur Folge, dass der Sachverhalt mit den dem TLfDI zur Verfügung stehenden Untersuchungsbefugnissen aus Art. 58 Abs. 1 DS-GVO in

Verbindung mit § 7 Abs. 1 Satz 1 und Abs. 2 ThürDSG nicht eindeutig aufklärbar war.
Einen naheliegenden beziehungsweise sich aufdrängenden Datenschutzrechtsverstoß, der zur Folge hätte, dass sich der TLfDI hinsichtlich seines Auswahlermessens nur eines bestimmten Instruments seiner Abhilfebefugnisse aus Art. 58 Abs. 2 DS-GVO hätte bedienen können (Ermessensreduktion auf Null), konnte der TLfDI aber gerade nicht feststellen. Zum einen konnte er die Ausführungen der Stadt mit den ihm zur Verfügung stehenden Aufklärungsbefugnissen nicht widerlegen, zum anderen erachtete der TLfDI den Sachvortrag der Stadt, den Verdacht der Scheinehe des Herrn X mittels seines auf einer Social Media Plattform geposteten öffentlich einsehbaren Status des Familienstandes nachzuweisen, für plausibel.
Die zugrundeliegende Beschwerde wies der TLfDI somit als unbegründet zurück.
Der Beschwerdeführer machte in diesem Fall von seiner Klagemöglichkeit gegen den Bescheid des TLfDI Gebrauch und erhob beim Verwaltungsgericht Weimar Klage gegen den Bescheid des TLfDI. Das Gericht sah für die Klage aber keine Aussicht auf Erfolg. „Der Kläger hat nur einen Anspruch auf ermessensfehlerfreie Entscheidung, nicht auf ein konkretes behördliches Handeln“, so das Verwaltungsgericht Weimar im Rahmen des mündlichen Erörterungstermins (Az.: 3 K 1490/21 We).
Ermessensfehler des TLfDI sah das Gericht nicht. Dies führte dazu, dass der Rechtsanwalt des Beschwerdeführers seinen Klageantrag zurücknahm und der Fall damit für den TLfDI beendet war.

2.4 Private E-Mail-Adressen eines Bürgermeisters sind nur eins: privat!

Ein Bürgermeister darf – wie alle Funktionsträger und Mitarbeiter öffentlicher Stellen – E-Mails, die er in seiner Funktion als Bürgermeister erstellt, ausschließlich über seine dienstliche Funktions-E-Mail-Adresse versenden. Er hat beim Versand durch geeignete technische und organisatorische Maßnahmen die Integrität und die Vertraulichkeit sicherzustellen und insbesondere zu prüfen, ob die Empfängeradressen eine angemessene Sicherheit gewährleisten, Art. 5 Buchstabe f), Art. 32 Abs. 1 DS-GVO. Andernfalls liegt ein datenschutzrechtlicher Verstoß vor, der, wie im konkreten Fall nach Art. 58 Abs. 2 Buchstabe b) DS-GVO, zu verwarnen ist.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Beschwerde vor, wonach der ehrenamtliche Bürgermeister einer Thüringer Gemeinde dienstlichen Schriftverkehr über seine private E-Mail-Adresse geführt und diesen an ebenfalls private E-Mail-Adressen weitergeleitet haben sollte. Konkret seien an eine weitere Thüringer Behörde E-Mails von der privaten E-Mail-Adresse des Bürgermeisters geschickt worden, die personenbezogene Daten des Beschwerdeführers enthielten. Der Bürgermeister habe diese E-Mails zudem an unbeteiligte Privatpersonen weitergeleitet.
Der Beschwerdeführer legte dem TLfDI zum Nachweis Ausdrucke von acht E-Mails vor, von welchen er im Rahmen einer Akteneinsicht Kenntnis erlangt hatte.
Der TLfDI ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nach Art. 51 Datenschutz-Grundverordnung (DS-GVO) Aufsichtsbehörde für die Thüringer Gemeinden. Im Rahmen der Anhörung der Gemeinde gemäß § 7 Abs. 1 Satz 2 ThürDSG in Verbindung mit § 28 Abs. 1 Thüringer Verwaltungsverfahrensgesetz konnte der TLfDI den Sachverhalt dahingehend aufklären, dass die Personen, an welche die E-Mails von dem Bürgermeister weitergeleitet wurden, keineswegs als Privatpersonen fungierten. Vielmehr übten sie öffentliche Funktionen aus, die im Zusammenhang mit dem dem E-Mail-Verkehr zugrundeliegenden Sachverhalt standen und die somit informiert werden durften. Die Gemeinde konnte umfassend für die jeweiligen Personen die sachlichen Grundlagen für die Übermittlung darlegen. Somit war den Anforderungen des Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) DS-GVO in Verbindung mit § 16 Abs. 1 ThürDSG Genüge getan. Hiernach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
Jedoch hatte der Bürgermeister seine private E-Mail-Adresse zum Versand von E-Mails mit personenbezogenen Daten des Beschwerdeführers genutzt und nicht geprüft, ob es sich bei den Empfänger-E-Mail-Adressen um private E-Mail-Adressen gehandelt haben könnte. Die Gemeinde erklärte, die E-Mail-Adressen der Empfänger seien ihr von einer anderen öffentlichen Stelle mitgeteilt worden.
Der TLfDI stellte fest, dass es sich teilweise um dienstliche E-Mail-Adressen handelte. Teilweise übersandte der Bürgermeister jedoch

personenbezogene Daten des Beschwerdeführers an private und (privat-) geschäftliche E-Mail-Adressen, in einem Fall an eine info@-Firmenadresse. In der Art und Weise der Übersendung der personenbezogenen Daten des Beschwerdeführers lag deshalb eine Verletzung von Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO aufgrund der Nichteinhaltung des Vertraulichkeitsgebots vor.

Gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Gemäß Art. 32 Abs. 1 DS-GVO treffen der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen gemäß Art. 32 Abs. 1 Buchstabe b) DS-GVO gegebenenfalls die Fähigkeit ein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Bei der Übermittlung an eine private E-Mail-Adresse ist grundsätzlich die Vertraulichkeit gefährdet. Es besteht die Gefahr, dass unbefugte Personen einen Zugriff auf die personenbezogenen Daten erhalten können. Zu nennen wären hier insbesondere die beteiligten E-Mail-Provider, welche durch die gewählte Übertragung Einsicht in den Inhalt der besagten E-Mails erhalten können. Ferner kann nicht vom Vorliegen der notwendigen technisch-organisatorischen Voraussetzungen zur Absicherung personenbezogener Daten ausgegangen werden.

Im vorliegenden Fall hatte der Bürgermeister die personenbezogenen Daten des Beschwerdeführers an private E-Mail-Adressen versandt. Somit war die Vertraulichkeit der personenbezogenen Daten nicht gegeben.

E-Mails sind schon standardmäßig nicht zwingend Ende-zu-Ende-verschlüsselt und daher hinsichtlich der Vertraulichkeit vergleichbar mit einer Postkarte. Selbst mit aktivierter Transportverschlüsselung haben die am Versand und Empfang der E-Mail beteiligten E-Mail-Provider Zugriff auf die Inhalte im Klartext. Neben der Bereitstellung des Dienstes haben E-Mail-Provider als eigenständige Verantwortliche häufig noch weitere Verarbeitungszwecke. Durch die Nutzung der privaten und (privat)geschäftlichen E-Mail-Adressen sind die E-Mail-Provider an der Datenverarbeitung im Rahmen eines (privat)geschäftlichen Vertrages beziehungsweise privaten Nutzungsvertrages eingebunden. Die Konditionen und Verarbeitungszwecke im Rahmen der Verträge sind unklar und nicht durch eine öffentliche Stelle veranlasst. Selbst wenn durch Nutzung von Ende-zu-Ende Verschlüsselung die E-Mail-Provider daran gehindert werden würden, ihre zusätzlichen Verarbeitungszwecke durchzuführen, wäre der Empfang der E-Mails auf Privatgeräten der Beteiligten nicht auszuschließen. Eine Prüfung dahingehend sowie bezüglich des Sicherheitsniveaus solcher nichtdienstlichen Geräte hatte die Gemeinde nicht behauptet und wäre wohl auch nicht zu realisieren gewesen. Die Verarbeitung dienstlicher E-Mails auf privaten Geräten könnte jedoch gegen Art. 32 DS-GVO verstoßen. Dies hatte die Gemeinde nicht ausgeschlossen, bevor sie die E-Mails versandte.

Der Einsatz einer Transportverschlüsselung bietet einen Basis-Schutz und stellt einen Mindeststandard selbst bei wenig sensitiven personenbezogenen Daten zur Erfüllung der gesetzlichen Anforderungen dar, siehe hierzu auch die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 (Stand: 16. Juni 2021): https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

Ist über die Transportverschlüsselung beim Empfänger nichts bekannt und soll auf einen E-Mail-Versand dennoch nicht verzichtet werden, so ist der sichere Transport wenigstens durch entsprechende Konfiguration des sendenden Mail Transfer Agent (MTA) sicherzustellen. Diese Einstellungen werden (En)Forced TLS, Mandatory TLS oder ähnlich genannt. Unterstützt die Gegenstelle kein TLS, dann wird der Verbindungsaufbau abgebrochen. Dies entspricht dem Stand der Technik.

Die Einhaltung der Anforderungen an die Transportverschlüsselung muss zudem auch nachgewiesen werden können.
Hinsichtlich der dienstlichen Adressen darf von technischen Sicherheitsvorkehrungen ausgegangen werden. Bei den privaten und (privat-)geschäftlichen E-Mail-Adressen hängt das technische Schutzniveau aber weithin von der willkürlichen Konfiguration der Nutzer und der Konfiguration der E-Mail Provider ab – ein Prüfmechanismus analog Art. 28 Abs. 3 Buchstabe h) DS-GVO liegt hier nicht vor. Der Schutz vor Fremdzugriffen kann hier nicht sichergestellt werden. Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der TR 03108-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten. Dies kann aber beim Versand an beliebige nichtdienstliche Adressen nicht sichergestellt werden.
Verantwortliche, die E-Mail-Diensteanbieter als Empfänger ihrer Nachrichten in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DS-GVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung der Systeme und Endgeräte an die Diensteanbieter ein. Eine solche Überprüfung ist aber beim Versand von personenbezogenen Daten an beliebige private E-Mail-Accounts nicht möglich.
Dass die Sicherheit bei den Anbietern überhaupt geprüft wurde, behauptete die Gemeinde nicht einmal. Als völlig unmöglich gestaltet sich zudem in der Regel die Beurteilung der Sicherheit des Endgerätes. Die Prüfung obliegt dem Verantwortlichen, hier der Gemeinde. Die Gemeinde kann die Verantwortlichkeit bei der Übermittlung nicht auf die Empfänger verschieben, vergleiche § 18 Abs. 1 Satz 1 ThürDSG.
Es entlastete die Gemeinde auch nicht, dass die E-Mail-Adressen zum Kontakt von anderen bereitgestellt worden waren. Vielmehr obliegt es der Gemeinde, eigenständig für die datenschutzkonformen Voraussetzungen zu sorgen. Im Zweifel ist der übliche Dienstweg über die Post zu wählen. Die Einhaltung von Recht und Gesetz – inklusive des unionsrechtlich geprägten Datenschutzrechts – wird nicht erst zur Aufgabe der öffentlichen Stelle, sobald Hinweise hierzu von übergeordneten Aufsichtsstellen ergehen.
Besonders problematisch war der Versand an eine info@-Firmenadresse. Hier ist neben den aufgezeigten technischen Unzulänglichkeiten

des Übertragungsweges zu beachten, dass der Aufbau der E-Mail-Adresse einen Zugriff diverser verschiedener Nutzer beim Empfänger auf die Nachricht erwarten lässt. Eine info@-Adresse bedeutet üblicherweise, dass E-Mails zentral für die gesamte Firma dort eingehen. Diese Nachricht richtete sich aber gerade nicht an die Firma und deren Mitarbeiter zur Kenntnisnahme, sondern nur an die einzelne Person in ihrer persönlich wahrgenommenen öffentlichen Funktion.
Soweit E-Mails im Einzelfall sogar auch vom privaten E-Mail-Account des Bürgermeisters versandt wurden und somit technisch-organisatorische Maßnahmen teils an beiden Enden des Versands fehlten, wurde der Verstoß von der Gemeinde eingeräumt. Hier kann ein Zugriff Dritter nicht ausgeschlossen werden, sodass die Amtsgeschäfte des Bürgermeisters in Form von dienstlichen E-Mails mit personenbezogenen Daten Dritten zugänglich werden können.
Soweit diese Adresse auch zum Empfang von E-Mails genutzt wurde, ist ebenfalls von der Zugriffsmöglichkeit durch Dritte auszugehen. Dies ist selbstverständlich für die Führung von Dienstgeschäften zu vermeiden.
Aufgrund der Zusicherung der Gemeinde, künftig keine E-Mails von und an Privataccounts zu verschicken, konnte der TLfDI davon ausgehen, dass die Verstöße bekannt und behoben waren. Er verzichtete daher auf eine entsprechende Anweisung gemäß Art. 58 Abs. 2 Buchstabe d) DS-GVO und verwarnte die Gemeinde gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO.

2.5 Entscheidung über die Auskunftserteilung nach Art. 15 DS-GVO durch Verwaltungsakt

Macht ein Betroffener bei einer Behörde seinen Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO geltend, muss die verantwortliche Behörde prüfen, ob sie die Auskunft erteilt. Bei der Entscheidung über den geltend gemachten Anspruch auf Auskunft oder Kopie nach Art. 15 Abs. 1 beziehungsweise 3 DS-GVO handelt es sich zumindest dann um einen Verwaltungsakt im Sinne des § 35 Satz 1 ThürVwVfG, wenn die Behörde den Antrag nach Prüfung der gesetzlichen Grenzen und Ausnahmen ganz oder teilweise ablehnen will. Soll hingegen dem Antrag der betroffenen Person entsprochen werden, ist die Erteilung der Auskunft beziehungsweise die Herausgabe der Kopie zwar ein Verwaltungsakt, da er aber den Adressaten begünstigt, besteht keine Begründungs- und Rechtsbehelfsbelehrungspflicht.

Handelt es sich bei der Entscheidung über die Auskunftserteilung nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) um einen Verwaltungsakt? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) schließt sich der vorherrschenden Rechtsprechung an und bejaht dies. Zwar ist sowohl die Erteilung der Auskunft als auch die Bereitstellung einer Datenkopie nach Art. 15 Abs. 1 beziehungsweise 3 Datenschutz-Grundverordnung (DS-GVO) als schlichtes Verwaltungshandeln zu qualifizieren. Diesem Realakt geht aber eine Entscheidung der Behörde über den geltend gemachten datenschutzrechtlichen Anspruch voraus, den die vorherrschende Rechtsprechung als feststellenden Verwaltungsakt qualifiziert (VG Bremen Urteil vom 22. Juni 2022, Aktenzeichen: 4 K 1/21, OVG Münster (NRW), Urteil vom 8. Juni 2021 – 16 A 1582/20, BVerwG, Urteil vom 16. September 2020 Aktenzeichen: 6 C 10/19).
Hierfür spricht, dass die DS-GVO zwar einen unmittelbaren Anspruch auf Auskunft und Kopie in Form einer gebundenen Entscheidung vorsieht, die Behörde hierüber aber auf der Grundlage eines gesetzlichen Prüf- und Abwägungsprogramms entscheidet. So hat beispielsweise der Thüringer Gesetzgeber in Anwendung der Öffnungsklausel des Art. 23 DS-GVO in § 21 Thüringer Datenschutzgesetz Ausnahmen und Zustimmungsvorbehalte geregelt, die eine Verhältnismäßigkeitsprüfung erfordern. Das Ergebnis dieser Prüfung wird dann rechtlich verbindlich in Form eines Verwaltungsakts festgestellt. Zu prüfen sind dabei mögliche Ausschluss- und Beschränkungstatbestände. Fraglich ist, ob auch in der Erteilung einer Auskunft oder der Bereitstellung einer Kopie eine verbindliche (Einzelfall-)Entscheidung der Behörde über den geltend gemachten datenschutzrechtlichen Anspruch zu sehen ist. Nach Auffassung des TLfDI ist dies zu bejahen. Da die Behörde mit der Auskunftserteilung dem Antrag der betroffenen Person entspricht, entfällt allerdings die Begründungspflicht (§ 39 Abs. 2 Nr. 1 Verwaltungsverfahrensgesetz [VwVfG]) und für einen Rechtsbehelf fehlt es an der nötigen Beschwer (Fehling/Kastner/Störmer/Schwarz, Verwaltungsrecht, VwVfG, § 35 RN 49. Auch nach Art. 12 Abs. 3 DS-GVO besteht die Positivantwort darin, dass der Verantwortliche die begehrte Information mitteilt beziehungsweise die Daten herausgibt (Kühling/Buchner/Bäcker, DS-GVO, Art. 15 RN 32; Paal/Pauly/Hennemann, DS-GVO, Art. 15 RN 52).

2.6 Gesundheitsdaten für die Auszahlung von Corona-Überbrückungshilfen bei der TAB

Die Vorlage von nicht anonymisierten Quarantänebescheiden der Mitarbeiter und Mitarbeiterinnen von Subunternehmen für einen Antrag auf Überbrückungshilfe III Plus ist ein erheblicher Verstoß gegen die Datenschutzbestimmungen, da in erster Linie Gesundheitsdaten nach Art. 9 DS-GVO in Verbindung mit Erwägungsgrund 35 der DS-GVO betroffen sind. Die Corona-Pandemie kann hier nicht als Ausnahmetatbestand für die Nichteinhaltung des Datenschutzes herhalten.

Der Inhaber eines Unternehmens (der Beschwerdeführer) wandte sich im Berichtszeitraum mit einer Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Beschwerdeführer trug vor, dass sein Antrag auf Überbrückungshilfe III Plus von der dafür zuständigen Bank abgelehnt worden sei, da nicht eindeutig nachgewiesen werden konnte, dass der Umsatzeinbruch individuell durch die Corona-Pandemie bedingt gewesen sei. Da der Beschwerdeführer als Antragsteller nicht direkt von Corona-Ausfällen betroffen war, habe er stichhaltig nachzuweisen, dass er im Förderzeitraum individuell von einem coronabedingten Umsatzeinbruch betroffen gewesen sei. Der Beschwerdeführer berief sich in seinem Antrag auf Überbrückungshilfe darauf, dass die Vorgewerbetreibenden beziehungsweise Subunternehmen, deren Tätigkeiten zuvor für Leistungen des Beschwerdeführers zwingend erforderlich waren, hohe Krankenstände in Kauf nehmen mussten und somit kein Personal zur Verfügung gestanden habe. Um dies nachzuweisen, habe die Bank den Beschwerdeführer gebeten, die Subunternehmer zu benennen und dementsprechend die behördlichen Quarantäneanordnungen der betroffenen Mitarbeiter beziehungsweise Mitarbeiterinnen einzureichen.
Zunächst ersuchte der TLfDI die betreffende Bank um eine Stellungnahme zum Sachverhalt. Daraufhin räumte die Bank gegenüber dem TLfDI die vom Beschwerdeführer vorgetragenen Punkte vollumfänglich ein, sprich das Verlangen der Vorlage nicht anonymisierter Quarantänebescheide der Mitarbeiterinnen und Mitarbeiter der Subunternehmen. Die Bank berief sich dabei auch darauf, dass sie bei der Gewährung der Corona-Hilfen an die Belastungsgrenze gestoßen sei, dazu eine besondere Stresssituation ihrer Mitarbeiterinnen und Mitarbeiter vorgelegen habe und sie zusätzlich auf die Zuhilfenahme einer

beauftragten Wirtschaftsprüfungsgesellschaft angewiesen war. All dies konnte der TLfDI nachvollziehen, denn hierbei handelte es sich um einen erheblichen Verstoß gegen die Datenschutzbestimmungen, da in erster Linie Gesundheitsdaten nach Art. 9 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit Erwägungsgrund 35 der DS-GVO betroffen waren. Nach Erwägungsgrund 35 sollten zu den personenbezogenen Gesundheitsdaten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person, unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.
Daher verwarnte der TLfDI die Bank nach § 58 Abs. 2 Buchstabe b) DS-GVO. Hier lag konkret eine Verletzung der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 Buchstabe a) Variante 1 DS-GVO in Verbindung mit Art. 9 Abs. 2 DS-GVO in Verbindung mit § 16 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) vor, indem die Bank die Vorlage nichtanonymisierter Quarantänebescheide der Subunternehmer forderte. Nach Art. 5 Abs. 1 Buchstabe a) Variante 1 DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden, das heißt, die personenbezogenen Daten müssen auf einer zulässigen Rechtsgrundlage und in rechtmäßiger Weise verarbeitet werden. Dafür müssen bei der Verarbeitung auch alle zusätzlichen Anforderungen und Pflichten beachtet werden, die sich aus der DS-GVO oder aus dem nach der DS-GVO zulässigen nationalen Recht ergeben.

Rechtmäßig ist eine Verarbeitung, wenn eine ausreichende Rechtsgrundlage im Unionsrecht oder im unionsrechtlich zulässigen mitgliedsstaatlichen Recht existiert.
Die Aufforderung zur Benennung der Firmennamen der Vorgewerke (Subunternehmen) erfolgte zum Zweck der Aufgabenwahrnehmung im öffentlichen Interesse gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e), Abs. 2 und 3 Buchstabe b) DS-GVO in Verbindung mit § 16 Abs. 1 ThürDSG: Bei der Bank handelte es sich um eine Anstalt öffentlichen Rechts, mithin um eine öffentliche Stelle nach dem ThürDSG. Nach § 16 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
Gemäß der Richtlinie des Freistaates Thüringen über die Gewährung von Soforthilfen als Billigkeitsleistungen für „Corona-Überbrückungshilfen für kleine und mittelständische Unternehmen“ (Dritte und Vierte Phase), einschließlich der Neustarthilfe und Neustarthilfe plus vom 17. Dezember 2021 in Verbindung mit den Vollzugshinweisen Überbrückungshilfe III plus vom 25. Juni 2021, konnte die Überbrückungshilfe III Plus als freiwillige Zahlung zur Sicherung der wirtschaftlichen Existenz gewährt werden, wenn Unternehmen, Soloselbstständige und Angehörige der Freien Berufe coronabedingt erhebliche Umsatzausfälle erleiden. Der Beschwerdeführer hatte gemäß Punkt 1.2 der FAQ zur Corona-Überbrückungshilfe III Plus vom Bundesministerium für Wirtschaft und Klimaschutz zu versichern und soweit wie möglich darzulegen, dass die ihm entstandenen Umsatzeinbrüche coronabedingt sind. Gemäß Punkt 1.2 der FAQ zur Überbrückungshilfe III Plus besteht die Möglichkeit, stichhaltig nachzuweisen, dass die Beschwerdeführerin individuell von einem coronabedingten Umsatzeinbruch betroffen ist. Der Umsatzeinbruch gilt gemäß Punkt 1.2 der FAQ dann als coronabedingt, wenn der Geschäftsbetrieb durch Quarantänefälle oder Corona-Erkrankungen in der Belegschaft nachweislich stark beeinträchtigt ist.
Hier war allerdings nicht die Belegschaft des Beschwerdeführers **selbst** von den Erkrankungen betroffen, sondern die Mitarbeiterinnen und Mitarbeiter von Firmen der vorgeschalteten Gewerke. Um eine Ablehnung des Antrages des Beschwerdeführers eventuell abzuwenden, war daher die Benennung der Firmennamen der Subunternehmer

zum Zweck der Aufgabenwahrnehmung, sprich der Prüfung des Antrags auf Überbrückungshilfe III, für die Bank erforderlich. Da seitens des Beschwerdeführers auch keine schriftliche Korrespondenz zwischen den Vertragspartnern, wie Absagen für die Aufträge, Bestätigungen des Bauleiters oder Ähnliches, vorgelegt wurden, war die Benennung der Firmen das einzige und mildeste Mittel zum Nachweis der coronabedingten Umsatzeinbußen.
Jedoch verstieß das Verlangen der Bank zur Vorlage von nichtanonymisierten Quarantänebescheiden von Mitarbeitern der Subunternehmen gegen die Regelungen des Datenschutzrechts. Bei den Quarantäneanordnungen handelt es sich um Gesundheitsdaten gemäß Art. 9 Abs. 1 DS-GVO sowie im Sinne von Erwägungsgrund 35 der DS-GVO. Danach zählen zu den personenbezogenen Gesundheitsdaten alle Daten, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Die Verarbeitung von Gesundheitsdaten darf nur in den engen Grenzen des Art. 9 Abs. 2 DS-GVO in Verbindung mit § 16 Abs. 2 ThürDSG erfolgen. Ein solcher Ausnahmetatbestand und damit eine Rechtsgrundlage lag für die Vorlage der nichtanonymisierten Quarantäneanordnungen von Mitarbeiterinnen und Mitarbeitern der Subunternehmer im vorliegenden Fall nicht vor. Milderes Mittel wäre hier die Vorlage von anonymisierten Quarantänebescheiden oder eine Bestätigung der Subunternehmen vom Kranken- und Quarantänestand im betroffenen Zeitraum gewesen. Damit wäre dann dem Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchstabe a) Variante 1 DS-GVO in dem gebotenen Umfang Rechnung getragen gewesen. Der Vorgang konnte mit der Verwarnung der verantwortlichen Bank durch den TLfDI abgeschlossen werden.

2.7 Was darf die Schule in der Klasse zu einzelnen SchülerInnen verkünden?

Wer in der Schule durch eine Prüfung fällt, darf darauf vertrauen, dass das Prüfungsergebnis nicht den Klassenkameraden zur Kenntnis gegeben wird – weder durch offenes Verlesen der Note noch durch Bekanntgabe, ob die Prüfung bestanden oder nicht bestanden wurde. Dabei kommt es nicht darauf an, dass die Note verkündet wurde, auch

eine besondere „Behandlung“ des unglücklichen Prüflings, die auf ein entsprechendes Ergebnis schließen lässt, ist nicht zulässig.

Die Besondere Leistungsfeststellung, kurz BLF, die Gymnasiasten in Thüringen in der 10. Klasse absolvieren müssen, ist eine gefürchtete Prüfung. Wer sie nicht besteht, hat zwar eine zweite Chance in der Nachprüfung, doch wer auch hier einen schlechten Tag erwischt, für den heißt es zunächst: Ende mit der schulischen Laufbahn und statt des ersehnten Abiturs einen Regelschulabschluss.
Dass die Nerven bei der Verkündung der Prüfungsergebnisse bei vielen Beteiligten blank liegen, ist daher nachvollziehbar. Weitgehend bekannt an den Thüringer Schulen dürfte mittlerweile die Tatsache sein, dass Noten nicht vor der Klassenöffentlichkeit verkündet werden dürfen, da es sich dabei um personenbezogene Schülerdaten handelt, für deren Offenlegung es grundsätzlich keine Rechtsgrundlage gibt.
Im vorliegenden Beschwerdefall gaben die Eltern eines Schülers auch an, dass die Prüfungsergebnisse durch die Klassenlehrerin in schriftlicher Form an die Schülerinnen und Schüler ausgehändigt wurden. Während die Lehrerin die Umschläge mit den Ergebnissen verteilte, kündigte sie vor der Klasse an, dass diejenigen, die die Prüfung nicht bestanden hätten, zu einem Beratungsgespräch und zur Anmeldung der Nachprüfung zum Oberstufenleiter gehen müssten.
Nachdem sich die erste Welle der Erleichterung und Enttäuschung im Klassenraum gelegt hatte, forderte die Lehrerin eine Schülerin und einen Schüler auf, mit ihr gemeinsam das Klassenzimmer zu verlassen. Diesen beiden Jugendlichen verkündete sie dann gemeinsam vor der Tür des Klassenzimmers, dass sie nun mit ihnen zum Oberstufenleiter zur angekündigten Beratung und Nachprüfungsanmeldung gehen würde.
Dieses Vorgehen stellt zwar keine unmittelbare Bekanntgabe des Prüfungsergebnisses vor der Klassenöffentlichkeit dar, dennoch waren zumindest sehr leicht Rückschlüsse für die anwesenden Mitschülerinnen und Mitschüler dahingehend zu ziehen, dass die beiden Schüler, die mit der Lehrerin den Klassenraum verlassen mussten, die BLF nicht bestanden hatten. Offengelegt wurde das Prüfungsergebnis des Sohnes der Beschwerdeführer jedoch mindestens gegenüber der Mitschülerin, der ebenfalls vor der Tür des Klassenraumes gesagt wurde, dass sie die BLF nicht bestanden habe und daher von der Lehrerin zum Oberstufenleiter begleitet wurde.

Noten und Prüfungsergebnisse (auch „bestanden“ beziehungsweise „nicht bestanden“) sind personenbezogene Schülerdaten gemäß Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO), für deren Verarbeitung es einer Rechtsgrundlage bedarf. Gemäß § 57 Abs. 1 Thüringer Schulgesetz ist eine Verarbeitung personenbezogener Daten jedoch nur dann zulässig, wenn dies zur Wahrnehmung einer schulischen Aufgabe erforderlich ist. Im geschilderten Fall war die Separierung der durchgefallenen Schülerin und des Schülers im unmittelbaren Anschluss an die Übergabe der schriftlichen Ergebnisse und die Information, dass die durchgefallenen Schüler zur Beratung zum Oberstufenleiter gehen sollten, sowie die gleichzeitige Begleitung der beiden durchgefallenen Schüler zum Oberstufenleiter nicht zur Aufgabenerfüllung notwendig; hier hätte ein Verfahren gewählt werden müssen, das es den beiden Durchgefallenen ermöglicht hätte, den Beratungstermin gegebenenfalls auch in Begleitung eines Vertrauens- oder Klassenlehrers so wahrzunehmen, dass sie selbst über eine mögliche Kenntnisnahme des Termins durch die Klassenkameraden hätten entscheiden können. Damit lag ein Verstoß gegen die DS-GVO vor.
Die Schulleitung wurde vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Stellungnahme aufgefordert und gab an, den geschilderten Verstoß nachvollziehen zu können. Es wurde zugesichert, das Verfahren für die Zukunft so zu verändern, dass Rückschlüsse auf die Prüfungsergebnisse nicht mehr möglich seien – es sei denn die Schülerinnen und Schüler machen diese selbst öffentlich.
Die Schulleitung als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO wurde gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO durch den TLfDI verwarnt.

2.8 Digitales macht auch vor den Kitas nicht Halt

Bei der Nutzung von Kita-Apps werden in der Regel auch personenbezogene Daten von Kindern verarbeitet, die unter besonderem Schutz stehen. Sollen dazu noch Gesundheitsdaten wie die Anzahl der Toilettengänge und Schlafenszeiten in der App aufgenommen werden, gilt besondere Vorsicht bei der Frage, welche Rechtsgrundlage hierfür besteht und welche technischen und organisatorischen Maßnahmen getroffen werden müssen, um das hohe Risiko der Verletzung der Persönlichkeitsrechte der Kinder auszuschließen.

Fahrkarten, Heizung, Einkäufe, selbst die elektrische Zahnbürste kann heute über eine App gesteuert werden. Da erscheint es nur logisch, dass diese Technik zunehmend auch in den Kitas Einzug hält. Die Daten, die hier fließen, sind jedoch nicht zu vergleichen mit denen anderer App-Anwendungen, schließlich geht es nicht nur um personenbezogene Daten von Kindern, die nach der Datenschutz-Grundverordnung (DS-GVO) einen besonderen Schutz genießen, sondern möglicherweise zusätzlich auch um Gesundheitsdaten der Kinder, deren Verarbeitung gemäß Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt ist.

Die Zahl der App-Anbieter für die Zwecke der Kita-Organisation, Platzvergabe und zum Informationsaustausch mit den Eltern ist mittlerweile unübersichtlich groß; den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichen daher immer wieder Anfragen besorgter Eltern, ob die von der jeweiligen Kita genutzte App datenschutzkonform ist. Häufig sind diese Anfragen auch verbunden mit dem Hinweis, dass vor Einführung der App keine Einwilligung der Sorgeberechtigten eingeholt wurde.

Im hier geschilderten Fall war die Sachlage zusätzlich komplex, da die Software für den Betrieb der App durch die Stadtverwaltung angeschafft und der laufende Betrieb durch das Jugendamt finanziert wird, die Kitas, die die App nutzen, sich jedoch alle in freier Trägerschaft befinden. Außerdem wird mit der App zunächst die Kita-Platz-Vergabe organisiert, die Nutzung der App durch die Eltern ist damit im ersten Schritt nicht freiwillig, sondern verpflichtend („ohne App kein Kita-Platz“) und beruht auf der rechtlichen Verpflichtung der Stadt, Kinderbetreuungsangebote bereitzustellen (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit § 24 Sozialgesetzbuch – Achtes Buch (SGB VIII), § 3 Thüringer Kindergartengesetz und § 62 Abs. 3 und 4 SGB VIII. Die Stadt hat dabei ein nachvollziehbares Interesse, die Vergabe der Kita-Plätze möglichst effizient und damit aufwand- und kostensparend zu gestalten und ist in der Wahl einer entsprechenden digitalen Anwendung dafür – im Rahmen des datenschutzrechtlich Zulässigen – frei.

In einem zweiten Schritt, nämlich nach erfolgter Kita-Platz-Vergabe, ermöglicht die App einen Informationsaustausch zwischen der Kita und den Sorgeberechtigten. Die Verarbeitung der dabei erhobenen personenbezogenen Daten darf nur mit Einwilligung der Eltern erfolgen. Eine rechtliche Verpflichtung wie bei der Kita-Platz-Vergabe be-

steht in dieser Form für die Ausgestaltung des Informationsaustausches nicht. Selbst wenn nur Daten übermittelt werden, die nicht über rein organisatorische Angelegenheiten (wie die Information zu Terminen, Projekten und ähnlichem) hinausgehen, werden auch bei dieser Form der Nutzung die personenbezogenen Daten der Sorgeberechtigten verarbeitet. Sofern weitere personenbezogene Daten, insbesondere Daten der Kinder (Schlafzeiten, Toilettengänge et cetera) über die App ausgetauscht werden sollen, ist Vorsicht geboten. Daten der Kinder, die als Gesundheitsdaten gemäß Art. 9 Abs. 1 DS-GVO zu klassifizieren sind, dürfen nämlich nicht ohne Vorliegen eines besonderen Rechtfertigungstatbestandes gemäß Art. 9 Abs. 2 DS-GVO verarbeitet werden.

Gesundheitsdaten sind personenbezogene Daten, die auf die vergangene, gegenwärtige oder zukünftige körperliche oder geistige Gesundheit einer Person schließen lassen. Aus der Zahl der Toilettengänge und den Schlafdaten lassen sich zumindest mittelbar Rückschlüsse auf die körperliche Gesundheit eines Kindes schließen. Eine explizite Einwilligung in die konkrete Verarbeitung dieser Gesundheitsdaten sieht Art. 9 Abs. 2 Buchstabe a) DS-GVO zwar vor. Jedoch müssen Sorgeberechtigte dann vor Erteilung der Einwilligung auch hinreichend informiert werden, welche Daten ihrer Kinder zu welchen Zwecken verarbeitet werden. Beispielsweise müssen die Sorgeberechtigten auch darüber entscheiden können, ob Fotos, auf denen das eigene und andere Kinder zu sehen sind, auch anderen Eltern zugänglich gemacht werden können.

Der für die Datenverarbeitung Verantwortliche muss dafür einen detaillierten Einwilligungsbogen erstellen, der die genauen Kategorien der erhobenen personenbezogenen Daten und die Zwecke der Datenverarbeitung aufführt. Außerdem bedarf es des Hinweises, dass die Einwilligung freiwillig erfolgt und keine Nachteile entstehen, sofern sie nicht erteilt wird. Darüber hinaus müssen alle Informationen gemäß Art. 13 DS-GVO aufgeführt werden.

Unklar war im vorliegenden Fall, ob die Kita beziehungsweise der Kita-Träger selbst oder die Stadt Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist. Verantwortlich ist die Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der TLfDI wandte sich daher mit einem Auskunftsersuchen an die Stadt, bei der neben den Fragen zur Verantwortlichkeit auch weitere rechtliche Aspekte wie das Vorliegen eines Auftragsverarbeitungsvertrags sowie technische Fragen zur App beantwortet werden

mussten. Aus der Stellungnahme der Stadt war ersichtlich, dass im vorliegenden Fall die Stadt über die Einführung und den Anwendungsbereich der Software entschieden und die finanziellen Mittel zur Verfügung gestellt hatte. Daher ist die Stadt auch Verantwortliche für die Datenverarbeitung. Das Einholen der Einwilligung sowie die Erfüllung der Informationspflicht gemäß Art 13 DS-GVO liegt also bei der Stadt, wenngleich der Datenaustausch zwischen Kita und Sorgeberechtigten stattfindet. Zwischen dem Anbieter der App sowie zwischen der Stadt und der Kita lag ein entsprechender Auftragsverarbeitungsvertrag vor, der die rechtliche Voraussetzung dafür bildet, dass die Kitas die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten dürfen, selbstverständlich vorausgesetzt, es liegt zudem eine entsprechende Einwilligung der Sorgeberechtigten vor.
In technischer Hinsicht war darauf zu achten, dass keine personenbezogenen Daten in Drittstaaten außerhalb des Europäischen Wirtschaftraums, für die kein Angemessenheitsbeschluss nach Art. 45 Abs. 1 DS-GVO vorliegt, übertragen werden. Ein solcher Angemessenheitsbeschluss beinhaltet, dass die Europäische Kommission beschlossen hat, dass in diesem Drittland ein der europäischen Datenschutz-Grundverordnung entsprechendes Schutzniveau für personenbezogenen Daten besteht. Eine Übertragung von personenbezogenen Daten in einen Drittstaat ohne Angemessenheitsbeschluss lag bei der in diesem Fall genutzten App nicht vor, sodass insoweit gegen den Einsatz der App weder aus datenschutzrechtlicher noch aus technischer Sicht durchgreifende Bedenken bestanden.

2.9 Maskenpflicht in der Schule und wie man ein Nichttragen glaubhaft machen muss

Schulleiter sind keine Ärzte: Können sie dennoch medizinische Diagnosen auf Masken-Attesten prüfen? Falls nicht, dürfen sie diese zur Prüfung an das Schulamt weiterleiten? Eine gesetzliche Regelung, welche Gesundheitsdaten ein Attest zur Befreiung vom Tragen einer Mund-Nase-Bedeckung für Schülerinnen und Schüler enthalten muss und wie diese glaubhaft gemacht werden können, gab es in Thüringen nicht. Um Gefälligkeitsatteste auszuschließen, konnten dennoch datenschutzkonforme Möglichkeiten gefunden werden.

„Wir sind dabei, für unser Kind ein Maskenattest zu bekommen. Dieses liegt aber noch nicht vor und wir können auch nicht genau sagen, wann dies so sein wird. Wir möchten nach wie vor nicht, dass unser

Kind ganztägig eine Maske tragen muss!“ Mit dieser Formulierung wandten sich besorgte Eltern an eine Schulleiterin, die neben dem Hinweis auf das in der entsprechenden Rechtsverordnung geregelte Betretungsverbot für Schülerinnen und Schüler, die keine Maske tragen und kein Attest zur Befreiung davon vorlegen können, die Eltern auch darüber informierte, dass ein solches Attest eine medizinische Diagnose enthalten müsse und sie dieses durch das Schulamt prüfen lassen würde.
Erbost forderten die Eltern den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf, gegen die Schulleiterin vorzugehen, da nach ihrer Auffassung nicht nur die Diagnose auf dem Attest nichts zu suchen hätte, sondern auch die Weiterleitung des Attests an das Schulamt einen Verstoß gegen den Datenschutz darstelle.
Zum Zeitpunkt der Beschwerde galt die Verpflichtung zur Verwendung einer qualifizierten Gesichtsmaske gemäß § 6 Abs. 5 Nr. 2 der Thüringer Verordnung zur Regelung infektionsschutzrechtlicher Maßnahmen zur Eindämmung des Coronavirus SARS-CoV-2 (ThürSARS-CoV-2-IfS-MaßnVO) nicht für Personen, denen die Verwendung einer qualifizierten Gesichtsmaske wegen Behinderung oder aus gesundheitlichen oder anderen Gründen nicht möglich oder unzumutbar war; dies musste – so der Wortlaut der Rechtsverordnung – „in geeigneter Weise glaubhaft“ gemacht werden.
Zur Frage, in welcher Weise die Glaubhaftmachung erfolgen könne, hieß es in der Begründung zur Verordnung: „Dies kann z. B. durch das Vorweisen eines ärztlichen Zeugnisses, eine Ausnahmegenehmigung der für den jeweiligen Ausnahmetatbestand zuständigen Behörde oder eine glaubhafte Darlegung der Hinderungsgründe geschehen.“ Da keine konkreten Anforderungen an die Ausgestaltung eines ärztlichen Zeugnisses vom Gesetzgeber gestellt wurden (beispielsweise dazu, ob ein ärztliches Attest zur Vorlage bei der Schule eine Diagnose enthalten muss), musste der unbestimmte Rechtsbegriff „in geeigneter Weise“ ausgelegt werden.
Aus datenschutzrechtlicher Sicht gilt der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) Datenschutz-Grundverordnung [DS-GVO]), wonach die Verarbeitung personenbezogener Daten auf das für die Zwecke notwendige Maß zu beschränken ist. Danach musste das Attest nur so viel Informationen enthalten, wie zur Glaubhaftmachung erforderlich sind. Bei medizinischen Diagnosen handelt

es sich um besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DS-GVO, in diesem Fall um Gesundheitsdaten. Diese unterliegen einem besonderen Schutz und dürfen ohne Einwilligung der betroffenen Person nur unter ganz bestimmten, strengen Voraussetzungen verarbeitet werden (Art. 9 Abs. 2 DS-GVO).
Zur Ausgestaltung eines Attests zur Vorlage bei der Schule waren bereits mehrere gerichtliche Urteile ergangen. So hat das Verwaltungsgericht Würzburg für die Vorlage eines Attests bei der Schule am 16. September 2020 gefordert, dass die Angabe einer medizinischen Diagnose im ärztlichen Attest zur Befreiung vom Tragen einer Mund-Nasen-Bedeckung enthalten sein muss (Az. W 8 E 20.1301). In diesem Bereich (öffentlich-rechtlich) bekommen nur Personen Kenntnis von der Diagnose (Schulleitung, Gesundheitsamt), die dazu befugt sind und zudem der Amtsverschwiegenheit unterliegen. Allerdings regelte im Unterschied zur Thüringischen Verordnung die Bayerische Infektionsschutzmaßnahmenverordnung, dass ein solches Attest „konkrete Angaben zum Grund der Befreiung enthalten muss".
Zu einem ähnlichen Ergebnis kam auch das Oberlandesgericht Dresden in seiner Entscheidung vom 6. Januar 2021 (Az. 6 W 939/20). Danach müssen ärztliche Atteste, die vom Tragen eines Mund-Nasenschutzes befreien, nachvollziehbar dokumentieren, welche „konkreten gesundheitlichen Beeinträchtigungen aufgrund der Tragepflicht in der Schule alsbald zu erwarten sind und woraus diese im Einzelnen resultieren".
In Baden-Württemberg fehlten, vergleichbar wie in Thüringen, in der entsprechenden Verordnung konkrete Vorgaben zur Glaubhaftmachung eines Ausnahmetatbestandes. In Baden-Württemberg hat das Verwaltungsgericht Sigmaringen mit Urteil vom 22. Juni 2021 (Az. 4 K 1827/21) für die Anforderungen an ein ärztliches Attest zur Befreiung von der Maskenpflicht zur Vorlage bei der Schule Folgendes festgestellt:
„1. Die Glaubhaftmachung des Vorliegens eines Ausnahmetatbestands durch eine ärztliche Bescheinigung, die dazu berechtigt, die Schule ohne Maske zu besuchen, setzt grundsätzlich nicht voraus, dass ein qualifiziertes ärztliches Attest vorgelegt werden muss.
2. Bei der Prüfung des o.g. Ausnahmetatbestands ist einzustellen, dass die Corona-Verordnungen keine ausdrückliche Definition des Begriffs der ärztlichen Bescheinigung oder qualitative Vorgaben hierzu enthalten, der Rechtsverkehr ärztlichen Attesten grundsätzlich

eine gehobene Beweiswirkung zuspricht, die Preisgabe von Gesundheitsdaten besonders sensibel ist, dem Schüler grundsätzlich ein Recht auf Teilnahme am Unterricht zusteht, das derzeit durch die infektionsschutzrechtlich erforderlichen Maßnahmen überlagert wird, und der Schüler als polizeilicher Nichtstörer in Anspruch genommen wird."
Einige kreisfreie Städte und Landkreise in Thüringen hatten daher in Bezug auf die oben genannte Regelung in der ThürSARS-CoV-2-IfS-GrundVO eigene Allgemeinverfügungen erlassen und darin beispielsweise die Regelung getroffen, dass das ärztliche Attest zur Befreiung von der Maskenpflicht im zuständigen Gesundheitsamt vorgelegt werden und das Gesundheitsamt eine eigene Bescheinigung ausstellen musste, die die Kontraindikation zum Tragen einer Maske bestätigte. Die medizinische Diagnose war in diesem Falle nur der/dem befugten Mitarbeiter/in des Gesundheitsamtes nach dem Infektionsschutzgesetz (IfSG) vorzulegen. Sofern es sich um den Amtsarzt/ die Amtsärztin handelte, war diese/r zudem Berufsgeheimnisträger aufgrund § 203 Abs. 1 Strafgesetzbuch. Damit wurde der Schutz sensibler personenbezogener Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO sicher gewahrt.
Anhand dieser Erläuterungen riet der TLfDI den Eltern zu erwägen, die medizinische Diagnose ihres Kindes, wegen der es vom Tragen einer Mund-Nasen-Bedeckung befreit war, beim zuständigen Gesundheitsamt vorzulegen, eine behördliche Bescheinigung vom Gesundheitsamt über die Befreiung von der Maskenpflicht ausstellen zu lassen und diese in der Schule vorzulegen.
Außerdem gab der TLfDI den Beschwerdeführern den Hinweis, dass die Schule grundsätzlich nicht befugt ist, von Impfnachweisen und/oder ärztlichen Attesten, die medizinische Diagnosen des Kindes enthalten, Kopien anzufertigen, da dies datenschutzrechtlich nicht zulässig ist. Klassenlehrer beziehungsweise Schulleitungen dürfen Immunitäts- oder andere medizinische Nachweise (Impfpass und/oder ärztliches Attest) nur einsehen und sich einen entsprechenden Vermerk über die Vorlage machen. Lediglich dieser Vermerk über die Vorlage kann dann zur Schülerakte genommen werden.
Da zum Zeitpunkt der Beschwerde von den Eltern der Schule weder ein Attest vorgelegt, geschweige denn weitergeleitet wurde, bestand auch kein Verstoß gegen die Datenschutz-Grundverordnung. Mit den erteilten Informationen konnte ein solcher Verstoß bereits im Vorfeld vermieden werden.

2.10 OLG Karlsruhe zur Plicht, Angaben des Auftragsverarbeiters zu hinterfragen

Das OLG Karlsruhe erließ am 7. September 2022 einen Beschluss (Aktenzeichen 15 Verg 8/22), wonach in einem vergaberechtlichen Bieterverfahren bei der Vergabeentscheidung grundsätzlich davon ausgegangen werden kann, dass ein Bieter seine vertraglichen Zusicherungen (hier personenbezogene Daten DS-GVO-konform zu verarbeiten) erfüllen wird. Nur für den Fall, dass sich aufgrund konkreter Anhaltspunkte Zweifel ergeben, müsse der Auftraggeber den Sachverhalt weiter prüfen. Die Erwartung einiger Schulen und Medien, dass diese Entscheidung der Freibrief für die Nutzung von Microsoft-Produkten im schulischen Bereich sei, musste der TLfDI enttäuschen. Zum einen bestehen gegen den Einsatz von Microsoft 365 in der Schule nicht nur „konkrete Anhaltspunkte für Zweifel“ an einem datenschutzkonformen Einsatz, sondern konkrete Beweise. Zum anderen bleiben die Schulen in der Verantwortung und damit Nachweispflicht, dass die verwendete Software nicht gegen EU-Datenschutzrecht verstößt – und das ist bezogen auf MS 365 derzeit schlichtweg nicht möglich!

Seit Jahren wird die Nutzung des Microsoft-Onlinedienstes MS 365 im öffentlichen Bereich, insbesondere bei der Nutzung an Schulen, durch die Datenschutzaufsichtsbehörden geprüft – mit unbefriedigendem Resultat. Trotz langer und intensiver Gespräche zwischen Vertretern der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), der Kultusministerkonferenz und der Microsoft Deutschland GmbH, bei denen umfangreiche technische und vertragsrechtliche Anforderungen gestellt und bewertet wurden, konnte kein grünes Licht für den schulisch veranlassten Einsatz gegeben werden. Auch im Ergebnis eines Pilotprojektes in Baden-Württemberg zur möglichen Einführung von Microsoft Office 365, jetzt Microsoft 365, an staatlichen Schulen, konnte weiterhin nicht sicher ausgeschlossen werden, dass die von Microsoft bei der Nutzung der Office-Produkte umfangreich erhobenen personenbezogenen Daten rechtswidrig für eigene Zwecke verarbeitet werden.
In Thüringen hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits zu Beginn der Corona-Pandemie die Schulleitungen darüber informiert, dass bei der

Nutzung von Microsoft 365 beziehungsweise des Videokonferenztools Microsoft Teams in jedem Fall ein Auftragsverarbeitungsvertrag gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) zwischen der Schule (Verantwortlicher im Sinne von Art. 4 Ziffer 7 DS-GVO) und dem Auftragsverarbeiter (hier Microsoft Deutschland GmbH) abgeschlossen werden müsste, der jedoch verschiedene gravierende Unklarheiten enthält, und legte seine datenschutzrechtlichen Bedenken zum schulisch veranlassten Einsatz von Microsoft-Produkten ausführlich dar. Das Thüringer Ministerium für Bildung, Jugend und Sport schloss sich der Rechtsauffassung des TLfDI an und untersagte als zuständiges Ministerium den Einsatz von Office 365 an den Schulen in Thüringen.

Mit großen Erwartungen war daher das Urteil des OLG Karlsruhe vom 7. September 2022 verbunden, in dem das Gericht festgestellt hatte, dass grundsätzlich davon auszugehen sei, dass ein Bieter seine vertraglichen Zusicherungen im Hinblick auf die Datenschutzkonformität seiner Verarbeitungen erfüllen wird. Gleich mehrere Anfragen von Schulen sowie entsprechende Veröffentlichungen in den Medien machten glauben, dass eine Zusicherung von Microsoft, personenbezogene Daten datenschutzkonform zu verarbeiten, nun ausreichen würde, um endlich den Startschuss für den Einsatz von MS 365 an Schulen zu geben.

Diese Hoffnung musste der TLfDI jedoch zunichtemachen und klärte die Sach- und Rechtslage für die Schulen dahingehend auf, dass die Entscheidung des OLG Karlsruhe nicht auf den Einsatz von Microsoft-Produkten in Thüringer Schulen übertragbar ist.

Das OLG Karlsruhe entschied in einem Vergabeverfahren. In Vergabeverfahren werden jedoch nicht vorrangig datenschutzrechtliche, sondern vergaberechtliche Kriterien geprüft. So hat das OLG in seiner Entscheidung ausgeführt, *„die Rüge, der Bieter setze einen Dienst ein, von dem aus Daten in die USA übertragen würden, auch werde die IP-Adresse in die USA übertragen, was der Bieter bestritten habe, ist wegen des im Vergabenachprüfungsverfahren im Interesse der Auftraggeber und der Allgemeinheit an einer raschen Auftragsvergabe geltenden Beschleunigungsgrundsatzes unbeachtlich.“* Datenschutzrechtlich ist so etwas undenkbar. Weiter führt das Oberlandesgericht aus, dass *„im Hinblick auf das Versprechen des Bieters, dass die Daten ausschließlich in Deutschland verarbeitet werden, es nicht darauf ankommt, ob der Bieter begleitende organisatorische und technische*

Maßnahmen, insbesondere auch im Hinblick auf eine sichere Verschlüsselung, zusagte, die erforderlich sind, damit die Übermittlung von Daten in die USA im Einklang mit den Bestimmungen der DS-GVO steht.“ Mit anderen Worten: Die eingesetzte Verschlüsselungstechnik wurde aus vergabeverfahrensrechtlichen Gründen nicht weiter geprüft. Für die Frage der datenschutzrechtlichen Zulässigkeit von Verarbeitungen spielt die Verschlüsselung jedoch eine zentrale Rolle. Aus der datenschutzrechtlichen Prüfung, die sich auf die Onlinedienste Microsoft 365 und Microsoft Education Office 365 (für Schüler und Lehrkräfte) bezieht, kann daher keine Zulässigkeit für die Nutzung dieser Produkte an Thüringer Schulen abgeleitet werden. Bereits aus den „vertraglichen Zusicherungen“ von Microsoft ergeben sich konkrete Anhaltspunkte dafür, dass die Bestimmungen der DS-GVO eben nicht eingehalten werden. Aus dem „Datenschutznachtrag“ zu den genannten Produkten ist ersichtlich, dass personenbezogene Daten in die USA oder andere Länder übermittelt werden. Außerdem gibt Microsoft an, diese Daten so offenzulegen, wie dies gesetzlich vorgeschrieben ist. Das kann also bedeuten, dass die personenbezogenen Daten gemäß US-amerikanischem Recht, etwa nach FISA (Section 702) oder Cloud Act, auf Anordnung lokaler Behörden von US-amerikanischen Unternehmen offengelegt werden müssen, unabhängig davon, wo sie gespeichert oder verarbeitet werden. Außerdem kann Microsoft nicht die notwendige Transparenz hinsichtlich einer Nutzung für eigene Zwecke bei der Auftragsverarbeitung herstellen und deren Rechtmäßigkeit nicht belegen. Dies nahm die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auch zum Anlass für ihre Festlegung zu MS 365, wonach „der Nachweis von Verantwortlichen, Microsoft 365 datenschutzkonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrages vom 15. September 2022‘ nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“ (https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf).

Verantwortliche, also die Schulleitungen, dürfen nur mit solchen Auftragsverarbeitern zusammenarbeiten, die Garantien dafür bieten, die Anforderungen der DS-GVO zu erfüllen (Art. 28 Abs. 1 und Erwägungsgrund 81 zur DS-GVO). Der Verantwortliche ist nach Art. 5

Abs. 2 DS-GVO für die Einhaltung des Abs. 1 (Grundsätze für die Verarbeitung personenbezogener Daten) verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“). Dies ist für Schulen aufgrund der oben genannten Problematik faktisch unmöglich.
Im Ergebnis ergibt sich für die Nutzung der MS 365-Produkte aus dem genannten Gerichtsbeschluss nichts Neues. Zum einen ist er für Thüringer Schulen nicht einschlägig, zum anderen können sich die Thüringer Schulen nicht darauf berufen, keine konkreten Anhaltspunkte für Zweifel an der Einhaltung von vertraglichen Zusicherungen zu haben, da die jahrelangen Prüfungen genügend Zweifel offengelegt haben. Der TLfDI hat bereits mehrfach auf die datenschutzrechtlichen Unzulänglichkeiten bei einer schulischen Nutzung von MS 365-Cloud-Produkten hingewiesen. Auch das Thüringer Ministerium für Bildung, Jugend und Sport hat seine Anordnung, dass Cloud-Produkte nichteuropäischer Anbieter für Unterrichtszwecke nicht genutzt werden dürfen, beibehalten.
Der Beschluss des OLG Karlsruhe vom 7. September 2022, 15 Verg 8/22, ist veröffentlicht unter: http://lrbw.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&nr=38130.

2.11 Heizkostenpauschale – wie kommen Studierende an ihr Geld?

Der TLfDI erteilt keine Freigabe zu geplanten Datenverarbeitungen. Er berät aber dazu, welche Anforderungen an eine datenschutzgerechte Verarbeitung zu stellen sind. So auch geschehen im Zusammenhang mit der Auszahlung der Heizkostenpauschale an Studierende.

Immer wieder treten Verantwortliche an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran und bitten um „datenschutzrechtliche Freigabe“ einer geplanten Datenverarbeitung. Die Datenschutz-Grundverordnung (DS-GVO) sieht aber eine derartige Freigabe durch die Datenschutzaufsichtsbehörde nicht vor. Vielmehr ist der Verantwortliche für die Einhaltung der datenschutzrechtlichen Vorgabe bei der von ihm vorgenommenen Verarbeitung personenbezogener Daten allein verantwortlich. Derartige Anfragen wertet der TLfDI als Beratungsanfragen.

So wurde es auch bei einer Anfrage des Thüringer Ministeriums für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) zum Heizkostenzuschuss gehandhabt.
Da die Preise für Energie am Weltmarkt stark gestiegen sind und so auch die Heizkosten in die Höhe getrieben wurden, hat die Bundesregierung Heizkostenzuschüsse für die einkommensschwächeren Haushalte beschlossen. Davon sollen auch Auszubildende, das bedeutet sowohl Studierende als auch Schülerinnen und Schüler, profitieren, die beim BAföG einen Wohnzuschlag oder beim Aufstiegs-BAföG (AFBG) einen Unterhaltsbeitrag erhalten. Das entsprechende Gesetz trat am 1. Juni 2022 in Kraft. Danach haben Anspruch auf einen einmaligen Heizkostenzuschuss
1. nicht bei den Eltern wohnende Auszubildende, denen Leistungen nach dem Bundesausbildungsförderungsgesetz für mindestens einen Monat im Zeitraum 1. Oktober 2021 bis 31. März 2022 bewilligt wurden, und
2. Aufstiegsfortbildungsteilnehmende, denen ein Unterhaltsbeitrag nach § 10 Abs. 2 des Aufstiegsfortbildungsförderungsgesetzes für mindestens einen Monat im Zeitraum 1. Oktober 2021 bis 31. März 2022 bewilligt wurde.
Das Vollzugsproblem für die Zuständigen vor Ort bestand darin, dass der Heizkostenzuschuss von Amts wegen geleistet werden sollte und kein Antrag erforderlich war.
Es wurde daher geplant, für die Auszahlung die Daten zu nehmen, die in dem Verfahren zur Erfassung, Bearbeitung, Bescheidung und Auszahlung von Leistungen nach der BAföG- beziehungsweise AFBG-Gesetzgebung bereits vorhanden waren (sogenanntes BAFSYS-Verfahren). Diese wurden zwar ursprünglich nicht zu diesem Zweck erhoben, allerdings waren im System alle personenbezogenen Daten vorhanden, um die Auszahlung der Heizkostenpauschale zu ermöglichen. Es war daher vorgesehen, dass durch Rechtsverordnung geregelt werden sollte, dass für die anspruchsberechtigten BAföG-Empfänger/innen die Ämter für Ausbildungsförderung – jeweils für ihren Zuständigkeitsbereich – auch für die Bewilligung des einmaligen Heizkostenzuschusses zuständig sein sollen.
Der TLfDI teilte dem TMWWDG mit, dass nach seiner Auffassung keine datenschutzrechtlichen Bedenken zu der beabsichtigten Vorgehensweise bei der Auszahlung von Heizkostenzuschüssen an BAföG-Empfänger bestünden. Nach § 1 Abs. 2 Nr. 1 des Gesetzes zur Ge-

währung eines einmaligen Heizkostenzuschusses aufgrund stark gestiegener Energiekosten (Heizkostenzuschussgesetz – HeizkZuschG) haben nicht bei den Eltern wohnende Auszubildende, denen Leistungen nach dem Bundesausbildungsförderungsgesetz für mindestens einen Monat im Zeitraum 1. Oktober 2021 bis 31. März 2022 bewilligt wurden, Anspruch auf einen einmaligen Heizkostenzuschuss. Dieser wird nach § 3 HeizkZuschG von Amts wegen ohne Antrag gewährt.
Das HeizkZuschG ist als Teil des Sozialgesetzbuches (SGB) zu verstehen, weil der Gesetzgeber es aufgrund seiner Zuständigkeit nach Art. 74 Abs. 1 Nr. 18 Grundgesetz (Wohngeldrecht) sowie aus Art. 74 Abs. 1 Nr. 13 Grundgesetz (Regelung der Ausbildungsbeihilfen) erlassen hat. Die Zulässigkeit der Nutzung der Daten musste sich daher aus dem SGB ergeben.
Bei der Ermittlung der Anspruchsberechtigten handelt es sich um eine Zweckänderung, die nach § 67c Abs. 2 Satz 2 Nr. 1 SGB X zulässig ist. Danach dürfen die im Rahmen der Aufgabenerfüllung gespeicherten Daten von demselben Verantwortlichen für andere Zwecke gespeichert, verändert oder genutzt werden, wenn die Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften dieses Gesetzbuches als diejenigen, für die sie erhoben wurden, erforderlich sind. Diese Voraussetzung ist gegeben, wenn, wie vorgesehen, in der Rechtsverordnung geregelt wird, dass für die anspruchsberechtigten BAföG-Empfänger/innen die Ämter für Ausbildungsförderung – jeweils für ihren Zuständigkeitsbereich – für die Bewilligung des einmaligen Heizkostenzuschusses zuständig sind. Andernfalls wäre das Tatbestandsmerkmal des gleichen Verantwortlichen nicht erfüllt.
Auf diese Weise wurde ermöglicht, dass den Anspruchsberechtigten ohne großen zusätzlichen Verwaltungsaufwand die ihnen zustehende Heizkostenpauschale ausgezahlt werden konnte.

2.12 Kontaktdaten für Studienzwecke

Art. 5 Abs. 1 Buchstabe a) DS-GVO fordert, dass personenbezogene Daten transparent und in einer für die Betroffenen nachvollziehbaren Art und Weise verarbeitet werden. Gemäß Art. 13 Abs. 1 DS-GVO in Verbindung mit Art. 12 Abs. 1 DS-GVO muss die/der Verantwortliche die betroffene Person umfassend und in verständlicher Art und Weise über die Verarbeitung ihrer Daten (Kontaktdaten der/des Verantwortlichen, Erhebungszwecke, Empfänger, Kategorien von Empfängern) informieren.

Im Februar 2022 wandte sich eine Beschwerdeführerin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie hatte sich in der Vergangenheit mit dem Corona-Virus infiziert und nun von einem Thüringer Klinikum ein Schreiben erhalten, in dem auf ihre Corona-Infektion Bezug genommen und sie gebeten wurde, ihre Einwilligung zur Teilnahme an einer medizinischen Studie zu erteilen. Im Schreiben des Klinikums wurde ausdrücklich Bezug auf das Gesundheitsamt genommen, das die Corona-Infektion der Beschwerdeführerin registriert hatte.
Bei positiven und negativen Testergebnissen über das Vorliegen oder Nichtvorliegen einer Infektion mit COVID-19 handelt es sich um personenbezogene Gesundheitsdaten, das heißt besondere Kategorien von Daten im Sinne von Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 15 Datenschutz-Grundverordnung (DS-GVO). Nach Art. 5 Abs. 1 Buchstabe f) DS-GVO sind diese Daten durch geeignete Maßnahmen vor dem Zugriff unbefugter Dritter zu schützen. Um festzustellen, ob das Gesundheitsamt tatsächlich personenbezogene Daten der Beschwerdeführerin unbefugt an das Klinikum übermittelt und auf welcher rechtlichen Grundlage die Beschwerdeführerin das Schreiben des Klinikums erhalten hatte, wandte sich der TLfDI mit einem entsprechenden Auskunftsersuchen an das zuständige Gesundheitsamt.
Das Gesundheitsamt teilte dem TLfDI mit, dass auch das Gesundheitsamt selbst bereits zahlreiche Nachfragen zum Schreiben des Klinikums erhalten hatte. Hintergrund für das Schreiben sei eine Studie des betreffenden Klinikums zu Langzeitfolgen einer Corona-Infektion gewesen. Das Klinikum hatte diesbezüglich das Gesundheitsamt um Kontaktdaten von positiv getesteten Personen gebeten. Die verantwortliche Stadt, der das Gesundheitsamt unterstellt war, hatte zugestimmt, die personenbezogenen (Adress-)Daten aller an Corona erkrankten Personen (4.600) für das beschwerdegegenständliche Anschreiben zu verwenden.
Die Verantwortliche teilte dem TLfDI mit, dass nur das Anschreiben an die Betroffenen einschließlich eines medizinischen Fragebogens vom Klinikum erstellt und an das Gesundheitsamt übergeben worden sei. Ein Mitarbeiter des Gesundheitsamtes jedoch habe dann entsprechende Serienbriefe erstellt und diese über die Poststelle der verantwortlichen Stadt an die Betroffenen, einschließlich die Beschwerdeführerin, versendet. Das Anschreiben an die Betroffenen enthielt aber nur den Kopfbogen des Klinikums und keinerlei Datenschutzhinweise

zur Verarbeitung der personenbezogenen Daten der Betroffenen gemäß Art. 13/14 (DS-GVO). Somit war für die Betroffenen nicht ersichtlich, woher die Klinik ihre personenbezogenen Daten über eine positive Corona-Infektion hatte und auf welcher Rechtsgrundlage gegebenenfalls das Gesundheitsamt die Daten (weiter-)verarbeitet hat.
Der TLfDI fragte nach, ob die verantwortliche Stadt aufgrund selbst erhaltener Nachfragen von Betroffenen zum Anschreiben des Klinikums gegebenenfalls eine allgemeine Information gemäß Art. 13 DS-GVO zur Verarbeitung der personenbezogenen Daten von Betroffenen und den Umständen des Klinikanschreibens veröffentlicht hatte, beispielsweise auf ihrer Internetseite oder im Amtsblatt. Die Verantwortliche teilte mit, dass sie keine Information an die Betroffenen über den Weg der Verarbeitung ihrer personenbezogenen Daten veröffentlicht und die Betroffenen diesbezüglich nicht informiert hatte.
Die Verarbeitung der personenbezogenen Daten der Beschwerdeführerin durch das Gesundheitsamt der Verantwortlichen verstieß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 13 Abs. 1 DS-GVO und Art. 9 Abs. 2 Buchstabe a) DS-GVO. Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten transparent und in einer für die Betroffenen nachvollziehbaren Art und Weise verarbeitet werden. Aufgrund des Briefkopfes vom Klinikum ließ das Anschreiben die Betroffenen nicht erkennen, dass es tatsächlich vom Gesundheitsamt der Verantwortlichen versandt worden war. Die Beschwerdeführerin und die Betroffenen wurden durch die Verantwortliche nicht gemäß den Vorgaben der DS-GVO umfassend in transparenter und verständlicher Form über die Verarbeitung ihrer personenbezogenen Daten informiert. Dies stellt einen Verstoß gegen das Gebot der transparenten und nachvollziehbaren Verarbeitung von personenbezogenen Daten gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 13 und Art. 12 Abs. 1 DS-GVO dar.
Im Rahmen der Anhörung des TLfDI nach § 28 Verwaltungsverfahrensgesetz räumte die Verantwortliche ein, dass die Abläufe im Prozess der Datenverarbeitung durch das Gesundheitsamt nicht optimal gewesen seien und eine Information nach Art. 13 DS-GVO zur Verarbeitung der personenbezogenen Daten der Betroffenen hätte ausgegeben werden müssen. Der TLfDI verwarnte die Verantwortliche wegen des Verstoßes gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 13 und Art. 12 Abs. 1 DS-GVO gemäß § 7 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit Art. 58 Abs. 2 Buchstabe b) DS-GVO im Dezember 2022.

2.13 Muss die Einstellungsbehörde von der ausbildenden Hochschule über alles informiert werden?

Für jede Datenübermittlung muss es eine Rechtsgrundlage geben. Das gilt auch für die Noten von Beamtenanwärtern. Sie dürfen nicht ohne Weiteres an die Einstellungsbehörde übermittelt werden.

Ein Beamtenanwärter einer Hochschule in Thüringen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er teilte mit, dass Ergebnisse von Probeexamen an die Einstellungsbehörden weitergeleitet werden.
Jede Verarbeitung von personenbezogenen Daten muss nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) rechtmäßig erfolgen. Die Übermittlung der Ergebnisse des Probeexamens durch die Hochschule bedarf daher einer Rechtsgrundlage.
Nach der Thüringer Ausbildungs- und Prüfungsordnung für die Laufbahn des gehobenen nichttechnischen Dienstes in der Kommunalverwaltung und der staatlichen allgemeinen Verwaltung (ThürAPOgD) werden die Anwärter im Vorbereitungsdienst sowohl in den Einstellungsbehörden als auch durch die Hochschule ausgebildet. Die Einstellungsbehörde ist nach § 3 Abs. 2 ThürAPOgD unter anderem zuständig für die Beaufsichtigung der Anwärter während der Ausbildung und sie weist die Anwärter der Hochschule zu. Weiterhin untersteht der Anwärter nach § 8 Abs. 2 ThürAPOgD der Dienstaufsicht der Einstellungsbehörde und während der Ausbildung an der Hochschule auch deren Dienstaufsicht. Nach § 11 ThürAPOgD führt die Einstellungsbehörde für jeden Anwärter eine Personalteilakte „Ausbildung“, in die neben dem Ausbildungsplan alle Leistungsnachweise und Bewertungen aufzunehmen sind.
Eine entsprechende Vorschrift zur Führung von Prüfungsunterlagen für die Fachhochschule zur Führung von Personalaktenunterlagen und Prüfungsakten findet sich nicht. Die Hochschule hat nach § 20 Abs. 5 ThürAPOgD nach Abschluss der Fachstudien Zeugnisse auszustellen, in denen die Leistungen des Anwärters im Haupt- und Abschlussstudium mit Punktzahlen und Noten aufgeführt werden. Insoweit muss auch die Hochschule über entsprechende Unterlagen zu den Anwärtern verfügen.
Nach den Vorschriften der ThürAPOgD sind Einstellungsbehörden von der Fachhochschule lediglich nach Abschluss der Fachstudien Zeugnisse über die Anwärter, in denen die Leistungen im Haupt- und

Abschlussstudium mit Punktzahlen und Noten aufgeführt werden, zu übermitteln.
Dies ist eine Übermittlungsvorschrift, die die Verarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe e) in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) rechtfertigt. Eine konkrete Übermittlungsvorschrift für andere Unterlagen zu erzielten Ergebnissen (zum Beispiel Probeexamen) findet sich hingegen im Gesetz nicht.
Die Hochschule ging davon aus, das Verfahren für die Studierenden/Anwärter transparent gestaltet zu haben, weil den Studierenden im Vorfeld eine entsprechende Information gegeben worden war. Allein die Information an die Studierenden, es werde eine Datenübermittlung an die Einstellungsbehörden über das Ergebnis erfolgen, ersetzt jedoch nicht die erforderliche Rechtsgrundlage für eine Übermittlung.
Anerkanntermaßen sind Schule und Ausbildungsbehörde für den erfolgreichen Abschluss der Ausbildung insgesamt verantwortlich, wobei die Verzahnung der Theorie und Praxis eine Abstimmung erforderlich macht und ein gleichgelagertes Interesse am erfolgreichen Abschluss vorliegt. Als Rechtsgrundlage für eine Übermittlung des Probeexamensergebnisses käme allenfalls noch § 17 Abs. 2 Nr. 4 Thüringer Datenschutzgesetz in Betracht. Danach ist die Verarbeitung von personenbezogenen Daten zu anderen Zwecken als zu denen sie erhoben wurden zulässig, wenn Dritte, an welche die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Voraussetzung wäre zunächst die glaubhafte Darlegung des Interesses durch die Einstellungsbehörde im Einzelfall oder aller Einstellungsbehörden an der Übermittlung gewesen, die nicht vorlag. Auch spricht viel dafür, dass die Studenten jedenfalls in Einzelfällen ein schutzwürdiges Interesse daran haben, dass die Einstellungsbehörde die Ergebnisse des Probeexamens nicht zur Kenntnis erhält.
Die Hochschule teilte mit, dass wegen der Änderung der ThürAPOgVwD die Übermittlung der Noten des Probeexamens an die Thüringer Ausbildungsbehörden seit 2021 nicht mehr stattfindet, weil durch die Neuorganisation des Studienablaufs die dargelegten Zwecke von der Ausbildungsbehörde, auf die Motivation der Anwärter kurz vor der schriftlichen Laufbahnprüfung Einfluss nehmen zu können, nicht mehr wahrgenommen werden können. Eine Übermittlung mit hinreichendem zeitlichem Vorlauf an die Einstellungsbehörden sei

nach den neuen Reglungen nicht mehr möglich. Insoweit seien weitere Übermittlungen von Probeexamensergebnissen aufgrund deren Wirkungslosigkeit eingestellt worden, der Datenschutzverstoß also für die Zukunft ausgeschlossen.
Der TLfDI sprach gegenüber der Hochschule nach Art 58 Abs. 2 Buchstabe b) DS-GVO eine Verwarnung aus, weil es in der Vergangenheit eine Datenübermittlung ohne Rechtsgrundlage gegeben hatte. Weitere Maßnahmen waren nicht erforderlich, da mit weiteren Verstößen nicht zu rechnen ist.

2.14 Darf der Personalrat Einblick in Lohnlisten haben?

Der Personalrat darf im Rahmen seiner allgemeinen Überwachungsbefugnis nach § 69 Abs. 1 ThürPersVG Einsicht in die Lohn- und Gagenlisten der Beschäftigten nehmen. Eine Einwilligung ist hierfür nicht erforderlich.

Eine öffentliche Stelle in Thüringen richtete die Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob der Personalrat ein Einsichtsrecht in Lohn- und Gehaltslisten von Künstlern, die nach Tarif bezahlt werden, ohne Einwilligung/Zustimmung der betroffenen Personen hat.
Als Rechtsgrundlage für die Einsicht in personenbezogene Daten und damit die Übermittlung als Verarbeitung an den Personalrat kommen Art. 6 Abs. 1 Satz 1 Buchstabe a) (Einwilligung der Betroffenen) oder Art. 6 Abs. 1 Satz 1 Buchstabe c) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) DS-GVO und einer spezialgesetzlichen Regelung in Betracht, nach dem die Verarbeitung personenbezogener Daten sowohl durch den Personalrat als auch durch die Dienststelle zulässig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt.
Maßgebliche Vorschriften für die Beteiligung des Personalrats sind die Vorschriften des Achten Teils des Thüringer Personalvertretungsgesetzes (§§ 66 bis 82b ThürPersVG). Zur Erfüllung der Aufgabe des Personalrats, nach § 66 Abs. 1 Nr. 2 ThürPersVG, dafür zu sorgen, dass die zugunsten der Beschäftigten geltenden Gesetze, hier insbesondere der Tarifverträge, durchgeführt werden, sind nach der Rechtsprechung (vergleiche BVerwG, Beschluss vom 16. Mai 2012,

6 PB 2.12) regelmäßig auch personenbezogene Lohn- und Gehaltslisten von Belang, sodass die Einsicht in die personenbezogenen Listen bejaht wird.
Zwar besteht nach den einschlägigen Tarifverträgen kein Mitbestimmungs- beziehungsweise Beteiligungsrecht des Personalrats zu personellen Entscheidungen. Das Recht zur Mitbestimmung oder die Beteiligung des Personalrats in den im ThürPersVG genannten Fällen ist jedoch bei der Erfüllung der allgemeinen Überwachungsbefugnis nach § 69 Abs. 1 ThürPersVG nicht Voraussetzung für die umfassende Unterrichtung zur Durchführung der Aufgaben.
Nach § 69 Abs. 1 ThürPersVG bestimmt der Personalrat nach Maßgabe dieser Vorschrift bei allen personellen Maßnahmen mit, die die Beschäftigten insgesamt, Gruppen oder einzelne Beschäftigte betreffen oder sich auf sie auswirken. § 69 Abs. 4 ThürPersVG regelt die Ausnahme, dass vorab die schriftliche Einwilligung der Betroffenen einzuholen ist, wenn Mitbestimmungsfälle über die beabsichtigten Maßnahmen hinaus schutzwürdige persönliche Interessen von Beschäftigten berühren. Dies ist jedoch auf die allgemeine Überwachungsbefugnis des Personalrats nicht übertragbar. Diese von der Einwilligung der betroffenen Beschäftigten abhängig zu machen, würde Sinn und Zweck der Vorschrift unterlaufen.
Der TLfDI kam nach Prüfung der dargelegten Aspekte zu der Auffassung, dass der Einsichtnahme in die Lohn- und Gagenlisten der Beschäftigten im Ergebnis keine datenschutzrechtlichen Vorschriften entgegenstehen.

2.15 Cyber-Sicherheitslage nach Angriff auf die Ukraine

Der Bericht zur „Lage der IT-Sicherheit in Deutschland 2022“ vom Bundesamt für Sicherheit in der Informationstechnik wird jährlich veröffentlicht. Verantwortliche von IT-Systemen sollten entsprechend den dort analysierten Risiken ihre eigene IT überprüfen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes legt jährlich einen umfassenden Bericht zur Lage der IT-Sicherheit in Deutschland vor.
Der Bericht „Lage der IT-Sicherheit in Deutschland 2022“ (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410) stand in die-

sem Jahr unter dem besonderen Eindruck des russischen Angriffskrieges auf die Ukraine. Denn in diesem Konflikt werden laut BSI nicht nur konventionelle Streitkräfte und Waffen, sondern auch digitale Angriffsmethoden eingesetzt. Seit Beginn des Angriffskriegs Russlands auf die Ukraine ist es in Deutschland zu einzelnen zusätzlichen IT-Sicherheitsvorfällen gekommen. So kam es laut BSI unter anderem mit dem Ausfall der satellitengestützten Kommunikation zur Fernwartung von Windenergieanlagen zu Kollateralschäden in Teilen Europas. Auch waren Betreiber Kritischer Infrastrukturen Angriffsziele von Cyber-Angriffen.
Aber auch die Bedrohung durch Cyber-Kriminelle hält an. So stieg die Bedrohung durch Cyber-Erpressung auf umsatzstarke Unternehmen an. Auch mehrere Kommunen waren in Deutschland 2022 betroffen, dadurch Verwaltungsprozesse teils über Monate massiv gestört. So meldete unter anderem auch die Stadtverwaltung Suhl im März 2022 dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) einen Cyber-Angriff, der die Verschlüsselung der Daten mit Lösegeldforderungen zur Folge hatte.
Weiterhin bargen die Schwachstellen, die 2022 bei MS Exchange bekannt wurden, ein hohes Angriffspotenzial.
Der TLfDI möchte dies zum Anlass nehmen darauf hinzuweisen, dass nach Einschätzung des BSI die Bedrohung im Cyber-Raum so hoch wie nie zuvor ist.
Es ist deshalb wichtiger denn je, alle Warnhinweise vom BSI sehr ernst zu nehmen (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Cyber-Sicherheitswarnungen/cyber-sicherheitswarnungen_node.html). Sie dienen zur Unterstützung der jeweiligen Sensibilisierungs-, Präventions- und Detektionsmaßnahmen. Halten Sie auch Ihre Betriebssysteme, Fachanwendungen, Antivirensoftwareprogramme immer auf dem aktuellen Stand der Technik. Überprüfen Sie auch Ihr Datensicherungsmanagement. Schulen Sie auch regelmäßig alle Mitarbeiter zu IT-Sicherheit und Datenschutz.

2.16 Protokollierung auf dem zentralen Internet-Server der Thüringer Landesverwaltung

Artikel 13 DS-GVO regelt die Informationspflicht bei der Erhebung personenbezogener Daten. Dies betrifft auch die Protokollierung bei

Zugriffen auf Webseiten. Auch diese Informationen sind aktuell und transparent darzustellen.

Die Datenschutz-Grundverordnung (DS-GVO) regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten erhoben werden. Bei der Informationspflicht im Falle der Direkterhebung wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO). Bei der Direkterhebung müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt beziehungsweise zur Verfügung gestellt werden. Dabei ist neben der Rechtsgrundlage und dem Zweck auch die Speicherdauer anzugeben. Näheres finden Sie dazu auch im Kurzpapier Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“ der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html.
Diese Informationspflichten müssen auch von Betreibern/Verantwortlichen von Webangeboten der Thüringer Landesverwaltung (ThLV) umgesetzt werden. Nicht nur, wenn sie beispielsweise über ein Kontaktformular personenbezogene Daten erfassen, sondern auch wenn in Protokolldateien die IP-Adresse gespeichert wird. Dies betrifft sowohl die Speicherung in Protokolldateien vor Ort als auch die Speicherung in Protokolldateien bei der Protokollierung des zentralen Internetzugangs durch das Thüringer Landesrechenzentrum.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) fragte deshalb beim Thüringer Landesrechenzentrum und beim Thüringer Finanzministerium (TFM) als fachlich zuständigem Ministerium zum aktuellen Stand zur Thematik Speicherfristen nach. Auch der TLfDI muss in seiner Datenschutzerklärung auf seiner Webseite die Informationspflichten aktuell halten, wenn personenbezogene oder personenbeziehbare Daten in Protokolldateien erfasst werden. Beim Zugriff auf die Internetseite des TLfDI wird zwangsläufig die IP-Adresse verarbeitet, um dem Thüringer Landesrechenzentrum technisch die Möglichkeit zu geben, die angeforderten Informationen (Text und Bilder der jeweiligen Seite) zur Ver-

fügung zu stellen. Die dabei anfallenden Verbindungsdaten (unter anderem auch die IP-Adresse) werden maximal vier Wochen gespeichert.
Dem TLfDI wurde ergänzend mitgeteilt, dass eine neue Richtlinie noch 2022 geplant sei und sich diese derzeit in Erarbeitung befinde. Bei der Einordnung der Thematik wurde zudem vom TFM erkannt, dass die Speicherfristen für die Verkehrsrichtung vom Internet auf Webangebote der Thüringer Landesverwaltung (ThLV) angepasst werden müssten, um eine effektivere Strafverfolgung bei Bedrohungen und Angriffen gegen die Landesverwaltung zu ermöglichen.
Der TLfDI bot und bietet ausdrücklich seine Bereitschaft zur Beratung bei der Thematik der neu zu treffenden erforderlichen Speicherfristen an, damit die Richtlinie zeitnah in Kraft tritt. Nicht zuletzt müssen auch die angeschlossenen Behörden des Corporate Network (CN) des Freistaats Thüringen ihrerseits in ihren Datenschutzhinweisen nach Art. 13 DS-GVO transparent die aktuelle Protokollierung beim Zugriff auf ihre Webseiten darstellen.

2.17 Wenn Straßenlaternen nicht nur leuchten

Auch bei Forschungsvorhaben hat der Verantwortliche entsprechend der Datenschutz-Grundverordnung die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten und die Sicherheit der Daten zu gewährleisten. Dies ist stets vor Projektstart zu prüfen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete in seinem Tätigkeitsbericht 2020 unter Nummer 2.14, dass die Bundesregierung Modellprojekte zu „Smart Citys“ fördert und diese seit 2019 in mehreren Staffeln auswählt.
Seit 2019 sind auch in Thüringen Modell- und Forschungsprojekte zum Thema „Smart City“ geplant. Der TLfDI berät in diesem Zusammenhang zu entsprechenden Forschungsprojekten. Dabei spielt auch das Thema künstliche Intelligenz beziehungsweise maschinelles Lernen immer wieder eine Rolle, da gerade hier große Potentiale von den Kommunen gesehen werden und auch hier ein besonders hoher Forschungsbedarf besteht.
Eine der Modellregionen fragte daher im Juli 2022 den TLfDI an, unter welchen Voraussetzungen es möglich sei, gewöhnliche Straßenla-

ternen durch „smarte Mikrofone“ so aufzurüsten, dass sich im Fall einer Gefahrenerkennung die Laterne einschaltet. Dazu sollten Mikrofone und nachverarbeitende Controller zum Einsatz kommen, welche sonst nur Lärmpegelmessungen durchführen. Die Idee war, dass die nachverarbeitenden Controller die aufgenommenen Geräusche klassifizieren können sollten, um Notsituationen zu ermitteln. Bei erkannten Notsituationen sollte ein Alarm an eine zentrale Stelle signalisiert werden und die Laterne sich einschalten. Die Erkennung von Notsituationen sollte durch maschinelles Lernen erfolgen. Da es ein solches System noch nicht marktfertig zu kaufen gibt, sondern hier lediglich an der Idee geforscht werden sollte, müssten auch Trainingsdaten für ein solches System aufgenommen und zunächst an zentraler Stelle gesammelt werden.

Für die datenschutzrechtliche Beurteilung dieses Projektes „intelligente Leuchten“ wurde der TLfDI angeschrieben. Es wurde davon ausgegangen, dass die aufgenommenen Geräusche auch personenbezogen sind, wie zum Beispiel menschliche Sprache mitsamt deren sprechertypischen Charakteristik sowie eventuell personenbezogenen Inhalten (Namen, Beschreibungen und so weiter). Obwohl in den meisten Fällen in den Audiodaten kein Personenbezug feststellbar sein dürfte (Auto, Hunde, Fluglärm), sind auch Fälle von Sprecheraufnahmen nicht selten. Der TLfDI vertrat unter Beachtung der Datenschutz-Grundverordnung (DS-GVO) folgende Auffassung: Erstens bedarf es einer Rechtmäßigkeit für die geplante Datenverarbeitung gemäß Art. 6 DS-GVO und zweitens sind die nötigen Sicherheitsmaßnahmen für die geplante Datenverarbeitung gemäß Art. 32 DS-GVO zu treffen. Um die Rechtmäßigkeit der Verarbeitung sicherzustellen, sieht die DS-GVO mehrere Möglichkeiten vor, wie zum Beispiel eine Einwilligung oder eine rechtliche Regelung oder die Wahrung öffentlichen Interesses. Eine Einwilligung scheidet als Rechtsgrundlage allerdings aus, da die Audioaufnahmen im öffentlichen Raum stattfinden sollten und vor Betreten des überwachten Gebietes potentiell von jeder Person diese eingeholt werden müsste. Problematisch ist, dass echte Hilferufe zum Training aufgenommen werden müssten und keine geschauspielerten Rufe, um eine echte Charakteristik zu erhalten.

Auf erneute Nachfrage zum Stand des Projektes teilte die Kommune dem TLfDI zwischenzeitlich mit, dass bis auf Weiteres Abstand vom Vorhaben genommen wird.

2.18 Weiterleitung von Beschwerden nur mit Rechtsgrundlage

Eine Meldung der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO ist dann nicht mehr angezeigt, wenn der Aufsichtsbehörde der Verstoß schon bekannt ist. Eine Weiterleitung von Beschwerden an Dritte bedarf einer Rechtsgrundlage. Bei der Weiterleitung an Arbeitgeber ist eine besonders sorgfältige Interessenabwägung erforderlich.

Eine betroffene Person beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ein Verantwortlicher ihre Beschwerde an einen Dritten weitergeleitet hatte. Dies hatte besondere Brisanz, da die betroffene Person sich über ihren Arbeitgeber beschwert hatte, über den der Verantwortliche nach Auffassung des Beschwerdeführers eine Kontrollfunktion ausübte. Prompt leitete der Verantwortliche die Beschwerde in nicht anonymisierter Form an den Arbeitgeber weiter.
Zu Recht verärgert, wandte sich der betroffene Arbeitnehmer an den TLfDI. Nachdem der Verantwortliche zur Stellungnahme aufgefordert worden war, meldete er das Vorgehen in diesem Fall als Verletzung des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-Grundverordnung (DS-GVO).
Da die Meldung nach Art. 33 DS-GVO erfolgte, allerdings zeitlich nach Zugang der Fragen des TLfDI aufgrund der vorliegenden Beschwerde des Betroffenen, hatte die Meldung nach Art. 33 DS-GVO grundsätzlich keinen Einfluss auf das Verwaltungsverfahren zur Beschwerdebearbeitung. Vielmehr hat das vereinfachte Verfahren in der Bearbeitung der Meldungen nach Art 33 DS-GVO nur dann abschließende Wirkung mit dem Ergebnis, dass grundsätzlich keine weiteren Maßnahmen nach Art. 58 Abs. 2 DS-GVO zu treffen sind, wenn die Meldung einer Beschwerde zuvorkommt. Dies war hier aber gerade nicht der Fall.
In der Sache legte der Verantwortliche dar, dass die bei ihm eingegangene Beschwerde an den Arbeitgeber weitergeleitet wurde, weil sie einerseits weder als vertraulich gekennzeichnet noch mit der Bitte versehen war, diese vertraulich zu behandeln. Andererseits hätte eine Interessensabwägung unter Berücksichtigung aller Umstände stattgefunden, bei der ein überwiegendes Interesses des Arbeitgebers festgestellt worden sei, da diesem die Rechtsverfolgung wegen unwahrer Behauptungen ermöglicht werden sollte.

Nach Auffassung des TLfDI kommt es nicht darauf an, ob eine Beschwerde als vertraulich gekennzeichnet oder mit der Bitte um vertrauliche Behandlung versehen ist. Personenbezogene Daten dürfen nur dann an Dritte übermittelt werden, wenn hierfür eine Rechtsgrundlage besteht, Art. 5 Abs. 1 Satz 1 Buchstabe a) DS-GVO. Eine solche war im vorliegenden Fall nicht erkennbar.
Der Verantwortliche hatte, anders als von dem Beschwerdeführer angenommen, keine Kontrollbefugnisse über den Arbeitgeber. Es handelte sich lediglich um eine Interessenvertretung. Dies hätte er dem Beschwerdeführer mitteilen und von einer weiteren Verarbeitung absehen müssen. Es war auch nicht erkennbar, dass dem Verantwortlichen eine besondere Fürsorge gegenüber seinen Mitgliedern im Zusammenhang mit Beschwerden gegen diese obliegt, selbst wenn Beschwerden schwerwiegende Anschuldigungen mit gegebenenfalls strafrechtlich relevantem Charakter enthalten. Für die Übermittlung der personenbezogenen Daten an den Arbeitgeber des Beschwerdeführers lag somit auch keine Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 DS-GVO vor.
Auch auf der Grundlage des Art. 6 Abs. 1 Satz 2 Buchstabe f) DS-GVO war eine Übermittlung nicht zulässig. Überwiegende Interessen des Arbeitgebers gegenüber der Beschwerdeführerin können nicht festgestellt werden. Dem Beschwerdeführer war nicht mitgeteilt worden, dass beabsichtigt war, die Beschwerde unter Angabe der Absenderadresse an den Arbeitgeber weiterzuleiten. Es empfiehlt sich jedoch, gerade im Rahmen der Abwägung mit den Interessen der betroffenen Person (auch) dieser Gelegenheit zur Äußerung zu geben, um deren Interessen zu konkretisieren, bevor es zu einer weiteren Verarbeitung der personenbezogenen Daten insbesondere durch Weitergabe an Dritte kommt. Die vorgenommene einseitige Abwägung war daher fehlerhaft, weil die Interessen des betroffenen Beschwerdeführers nicht beziehungsweise nicht ausreichend berücksichtigt wurden. Damit liegt ein Verstoß gegen Art 5 Abs. 1 Satz 1 Buchstabe a) in Verbindung mit Art. 6 Abs. 1 Satz 1 DS-GVO vor, weil es keine Rechtsgrundlage für die Datenübermittlung gab.
Der TLfDI sprach gegenüber dem Verantwortlichen eine Verwarnung aus.

3. Fälle nicht-öffentlicher Bereich

Erfolg Kurve Hand - Kostenloses Bild auf Pixabay

3.1 Videoüberwachung des Hauseingangs eines Mehrfamilienhauses

Die Inbetriebnahme einer Kamera, mit der die Überwachung des Eingangsbereichs eines Mehrfamilienhauses möglich ist, stellt einen erheblichen Eingriff in das allgemeine Persönlichkeits- und Selbstbestimmungsrecht der Mieter und deren Besucher dar. Aufgrund der regelmäßig nicht möglichen Einwilligungseinholung der unbestimmbaren Personen, welche sich im öffentlich zugänglichen Eingangsbereich aufhalten können, ist solch eine Videoüberwachung nur zulässig, insofern die Interessen des Kamerabetreibers gegenüber dem Persönlichkeitsrecht der betroffenen Personen überwiegen und keine milderen Mittel zur Erreichung des beabsichtigten Zwecks der Videoüberwachung zur Verfügung stehen.

Durch eine Ordnungswidrigkeitenanzeige bei der Polizei erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis darüber, dass ein Mieter eines Mehrfamilienhauses an seinem Balkon eine Videoüberwachungsanlage installiert hatte. Die Kamera war von dem Betreiber derart ausgerichtet,

dass dieser den Hauseingang sowie den daran vorbeiführenden Gehweg und angrenzende Teile des öffentlich zugänglichen Bereichs beobachten konnte. Das Verfahren wurde mit Übermittlung der Ordnungswidrigkeitenanzeige durch die Polizei zur Verfolgung einer Ordnungswidrigkeit an den TLfDI abgegeben.
Vor diesem Hintergrund wandte sich der TLfDI mit einer Anhörung an den Kamerabetreiber. Dieser teilte entgegen der Sachverhaltsdarstellung mit, dass es sich um einen Irrtum handelt, da er keine Kamera besitze und unter der Anschrift, an welcher sich die Kamera befindet, nicht gemeldet ist. Aufgrund dieser Aussage wandte sich der TLfDI mit einem Amtshilfeersuchen an die Polizei. Diese teilte dem TLfDI mit, dass durch eine Abfrage der Meldedaten des Betroffenen ermittelt werden konnte, dass dieser an der Anschrift, an welcher sich die Kamera befindet, wohnhaft ist. Zusätzlich konnten die Ermittlungen der Polizei durch zwei Zeugen bestätigt werden. Um den Sachverhalt abschließend prüfen zu können, vernahm der TLfDI die Zeugen ergänzend. Hierbei konnte ermittelt werden, dass die Kamera im Zeitraum der Prüfung des Tatvorwurfs abgebaut worden war.
Aufgrund der Aufrechterhaltung des Tatvorwurfs hatte der TLfDI im vorliegenden Fall zu prüfen, ob der Kamerabetreiber gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6 und 7 Datenschutz-Grundverordnung (DS-GVO) verstoßen hatte.
Die durch die Kamera aufgezeichneten Daten vom Betreten und Verlassen des Hauseingangs und dem Passieren des daran vorbeiführenden Gehwegs sowie Teilen des umliegenden öffentlichen Bereichs von einzelnen Personen sind als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO einzuordnen. Es ist davon auszugehen, dass Anwohner, Besucher sowie Angestellte und Passanten, die nicht damit rechnen mussten, gefilmt zu werden, in den Fokus der oben genannten Kamera geraten sind. Allein die Informationen darüber, wo sich eine bestimmte oder bestimmbare Person aufhält, mit wem sie sich trifft oder unterhält, ist eine Angabe über persönliche Verhältnisse, die mittels der Videoüberwachung erhoben wurde. Diese Daten sind nicht allgemein zugänglich. Aufgrund des unbestimmbaren Personenkreises, welcher sich im Bereich des Hauseingangs, des Gehwegs und des umliegenden öffentlichen Bereichs aufhalten konnte, ist die Einholung einer Einwilligung regelmäßig nicht möglich.
Es kam daher im vorliegenden Fall nur ein Erlaubnistatbestand für eine Datenverarbeitung durch die Kamera nach Art. 6 Abs. 1 Satz 1

Buchstabe f) DS-GVO in Betracht, soweit die Kamera zur Wahrnehmung der berechtigten Interessen des Kamerabetreibers erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der von der Videoüberwachung betroffenen Personen zum Schutz ihrer personenbezogenen Daten überwiegen. Die berechtigten Interessen können hierbei ideeller, wirtschaftlicher oder rechtlicher Natur sein. Ein berechtigtes Interesse wurde von dem Kamerabetreiber nicht dargelegt, wodurch zwingend von dem Überwiegen der Interessen oder Grundrechte und Grundfreiheiten der von der Videoüberwachung betroffenen Personen zum Schutz ihrer personenbezogenen Daten auszugehen war.
Durch die Überwachung des Hauseingangs, des daran vorbeiführenden Gehwegs und von Teilen des umliegenden öffentlichen Bereichs wurde erheblich in das Grundrecht der informationellen Selbstbestimmung nach Art. 6 Abs. 2 Thüringer Verfassung der videoüberwachten Personen eingegriffen. Durch die Videoüberwachung ist es möglich gewesen, Erkenntnisse über persönliche oder sachliche Verhältnisse einzelner natürlicher Personen zu erlangen, die sich – wenn auch nur zufällig – im Bereich der Überwachung aufhielten. Es konnten Bewegungsprofile erstellt werden. Weiterhin sind Rückschlüsse des Kamerabetreibers auf die Aufenthaltszeiten etwaiger Besucher nicht auszuschließen. Den Hauseingang sowie den daran vorbeiführenden Gehweg mussten alle Personen nutzen, die dort wohnten, arbeiteten oder zu Besuch waren. Eine Ausweichmöglichkeit war nicht gegeben. Insbesondere die Anwohner konnten der Videoüberwachung nicht ausweichen und waren stets dem von der Videoüberwachungsanlage ausgehenden Überwachungsdruck ausgesetzt.
Im Ergebnis konnte der TLfDI feststellen, dass die Interessen der von der Videoüberwachung betroffenen Personen überwogen hatten und somit eine unrechtmäßige Datenverarbeitung hinsichtlich der personenbezogenen Daten der Anwohner, etwaiger Besucher und Passanten, welche sich im öffentlich zugänglichen Aufnahmebereich befanden, vorgenommen worden war. Aufgrund des damit gegebenen Verstoßes gegen die Grundsätze für die Verarbeitung von personenbezogenen Daten, einschließlich der fehlenden Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6 und 7 DS-GVO wurde nach Art. 83 Abs. 5 Buchstabe a) DS-GVO eine Geldbuße gegen den Kamerabetreiber verhängt.

3.2 Veröffentlichung eines Fotos in einer Unternehmens-WhatsApp-Gruppe

Die „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO ist mit Verwendung des Begriffs „ausschließlich“ als Tatbestandmerkmal grundsätzlich eng auszulegen und erlaubt im Rahmen der Verarbeitung personenbezogener Daten keine Vermischung privater und beruflicher beziehungsweise wirtschaftlicher Belange. Wird daher eine interne WhatsApp-Gruppe von Beschäftigten eines Unternehmens als Kommunikationsmittel eingesetzt, ist der sachliche Anwendungsbereich der DS-GVO gemäß Art. 2 Abs. 1 DS-GVO eröffnet, wenn in der Gruppe nicht ausschließlich Nachrichten privater Natur versendet werden.

Mit einer Beschwerde nach Art. 77 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) wandte sich ein Rechtsanwalt im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und rügte für seinen Mandanten und Geschädigten die Verletzung der DS-GVO durch einen Mitarbeiter und Datenschutzbeauftragten eines in Thüringen ansässigen Unternehmens.
In diesem Zusammenhang berichtete der Rechtsanwalt, dass der betroffene Datenschutzbeauftragte des Unternehmens in einer internen WhatsApp-Gruppe des Unternehmens, welche inzwischen gelöscht worden war, ein Foto eingestellt hatte, welches den Geschädigten nach einem tätlichen Angriff stark blutend und mit ausgeschlagenem Zahn zeigte. Das Bild sei ohne Kenntnis des Geschädigten, welcher früher einmal selbst Mitarbeiter des Unternehmens gewesen sei, angefertigt und erst an ihn übermittelt worden, nachdem es in der WhatsApp-Gruppe veröffentlicht worden war.
Obgleich dem Datenschutzbeauftragten aufgrund dieses Verhaltens durchaus ein Mangel an Zuverlässigkeit zu unterstellen war, da er offensichtlich bewusst datenschutzrechtliche Bedenken hinsichtlich der Verwendung von WhatsApp im betrieblichen Kontext sowie Bedenken in Bezug auf die unrechtmäßige Veröffentlichung des Fotos ignoriert hatte, konnte seine Abberufung als Datenschutzbeauftragter durch den TLfDI nicht verlangt werden.
Gemäß § 40 Abs. 6 Satz 2 Bundesdatenschutzgesetz kann die Abberufung ausschließlich in den Fällen verlangt werden, in denen dem Datenschutzbeauftragten die erforderliche Fachkunde fehlt oder im

Falle des Art. 38 Abs. 6 DS-GVO ein schwerwiegender Interessenkonflikt vorliegt. Im vorliegenden Fall hatte der Geschäftsführer des Unternehmens gegenüber dem TLfDI jedoch nachgewiesen, dass der Datenschutzbeauftragte im datenschutzrechtlichen Kontext an zahlreichen Fortbildungsmaßnahmen und Qualifizierungen mit Erfolg teilgenommen hatte. Ein entsprechendes Verwaltungsverfahren war daher ohne das Ergreifen weiterer Maßnahmen abzuschließen.
Gleichwohl wurde hinsichtlich der Veröffentlichung des Fotos in der WhatsApp-Gruppe ein Bußgeldverfahren gegen den Datenschutzbeauftragten eingeleitet.
Im Rahmen der daraufhin durchgeführten Zeugenvernehmungen konnte durch den TLfDI ermittelt werden, dass das Foto im Rahmen eines bereits mehrere Jahre zurückliegenden Junggesellenabschieds entstanden war. Der auf dem Foto abgebildete Geschädigte hatte hierbei weder in die Anfertigung des Fotos noch in dessen Veröffentlichung eingewilligt. Dass der Datenschutzbeauftragte das Foto in die WhatsApp-Gruppe gestellt hatte, ließ sich zweifelsfrei belegen, nicht jedoch, dass dieser zugleich der Urheber des Fotos war. Der daraufhin angehörte Betroffene räumte die Veröffentlichung des Fotos ein, bestritt jedoch ausdrücklich, das Foto angefertigt zu haben.
Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen ihn.
Nach Art. 83 Abs. 5 Buchstabe a) DS-GVO handelt ordnungswidrig, wer gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9 DS-GVO verstößt. Insbesondere war vorliegend der sachliche Anwendungsbereich der DS-GVO eröffnet. Gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Eine solche Tätigkeit war hier jedoch gerade nicht anzunehmen, da die interne WhatsApp-Gruppe des Unternehmens unstreitig für die Kommunikation privater wie auch dienstlicher Belange genutzt worden war.
Da die „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO mit der Verwendung des Begriffs „ausschließlich“ als Tatbestandsmerkmal grundsätzlich eng auszulegen ist und daher nicht die Vermischung privater und wirtschaftlicher beziehungsweise geschäftlicher Tätigkeit erlaubt, gelangte diese vorliegend wegen der auch vorgenommenen Dienstkommunikation nicht zur Anwendung. Mit der Fotoaufnahme des Geschädigten wurden dessen personenbezogene

Daten im Sinne des Art. 4 Nr. 1 DS-GVO verarbeitet, da dieser auf dem Foto klar zu erkennen und damit identifizierbar war. Mit dem Einstellen des Fotos in die WhatsApp-Gruppe wurden personenbezogene Daten durch Übermittlung offengelegt und damit im Sinne des Art. 4 Nr. 2 DS-GVO verarbeitet. Die Verarbeitung dieser Daten erfolgte unrechtmäßig. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist.
Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt. Vorliegend konnte die Verarbeitung der personenbezogenen Daten nicht auf die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass der Geschädigte vor dem Einstellen seines Fotos in die WhatsApp-Gruppe unter Nennung des Zweckes in die Verarbeitung einwilligt hätte. Eine solche Einwilligung lag jedoch nicht vor. In diesem Zusammenhang konnte dahinstehen, ob der Geschädigte Kenntnis von der Existenz des Fotos hatte oder nicht, denn selbst wenn der Geschädigte damals seine Einwilligung in die Anfertigung des Fotos erteilt hätte, wäre hierin nicht zugleich eine Einwilligung in die Offenlegung zu sehen gewesen. Eine solche Einwilligung konnte auch nicht in der gegebenenfalls anzunehmenden stillschweigenden Duldung der Existenz des Fotos durch den Geschädigten gesehen werden. Gemäß Art. 4 Nr. 11 DS-GVO ist die Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder in einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Da insoweit eine eindeutige beziehungsweise aktive Handlung vorausgesetzt wird, stellt Schweigen oder Untätigkeit gerade keine Einwilligung dar (vergleiche Wortlaut Erwägungsgrund 32). Auch konnte die Verarbeitung der personenbezogenen Daten nicht auf den einzig noch in Betracht zu ziehenden Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden, da es bereits an einem berechtigten Interesse fehlte, welches von dem Betroffenen weder vorgetragen worden noch nach Aktenlage erkennbar war. In jedem Fall standen aber die schutzwürdigen Interessen des Geschädigten einer Übermittlung durch Offenlegung der personenbezogenen Daten entgegen. Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-

GVO musste durch den TLfDI zulasten des Betroffenen ein vorsätzliches Handeln berücksichtigt werden. Mildernd wirkte sich hingegen aus, dass der Datenschutzbeauftragte die rechtswidrige Datenverarbeitung eingeräumt hatte. Die in dem inzwischen rechtskräftigen Bußgeldbescheid festgesetzte Geldbuße im dreistelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.3 Rechtsanwalt erlangt rechtswidrig Daten durch die Staatsanwaltschaft – was nun?

Rechtsanwälte sind dazu angehalten, jede Verarbeitungstätigkeit von personenbezogenen Daten auf ihre Zulässigkeit hin zu prüfen. Eine gewährte Akteneinsicht in einem Gerichts- oder Strafverfahren bedeutet nicht, dass die aus diesem Verfahren erlangten Daten ohne Weiteres auch für weitere Verfahren beziehungsweise für Verfahren anderer Mandanten verwendet werden dürfen. Insbesondere, wenn diese Daten durch eine rechtswidrig erteilte Akteneinsicht erlangt wurden.

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde zur Durchsetzung eines Löschungsanspruchs gegenüber einem Rechtsanwalt. Der Beschwerdeführer hatte sich im Vorfeld der Beschwerde ohne Erfolg durch seine Rechtsvertreter an den betreffenden Rechtsanwalt gewandt. Aus der Beschwerde ergab sich folgender Sachverhalt:
Im Rahmen eines staatsanwaltschaftlichen Ermittlungsverfahrens wurde seitens des Rechtsanwalts für seine Mandantin – eine Bürgerinitiative – zusätzlich zu dem bereits von Amts wegen eingeleiteten Ermittlungsverfahren eine Strafanzeige wegen eines Umweltdelikts erstattet. Gleichzeitig beantragte er kurz vor Beendigung des Ermittlungsverfahrens Akteneinsicht bei der Staatsanwaltschaft. Die Staatsanwaltschaft führte die Bürgerinitiative als Anzeigeerstatterin und verletzte Person und gewährte die Akteneinsicht dem Rechtsanwalt als Vertreter der Bürgerinitiative nach Einstellung des Ermittlungsverfahrens der Staatsanwaltschaft.
Der hier die Löschung begehrende Beschwerdeführer legte als Beschuldigter in dem Verfahren Rechtsbehelf gegen die Entscheidung der Staatsanwaltschaft hinsichtlich der dem Rechtsanwalt der Bürgerinitiative gewährten Akteneinsicht ein. Das Landgericht entschied im

Beschwerdeverfahren durch Beschluss, dass die Akteneinsicht an den Rechtsanwalt rechtswidrig gewesen war, da es der Bürgerinitiative mangels Vorliegens eines Individualdelikts an der Verletzteneigenschaft fehle. Es lehnte jedoch einen Folgenbeseitigungsanspruch in Form der Löschung der Kopie der Akte bei dem Rechtsanwalt ab, da sich der Beschwerdeführer (Beschuldigte) aufgrund der Feststellung der Rechtswidrigkeit der Akteneinsicht selber behelfen könne.
Daraufhin wandten sich die Rechtsanwälte des Beschwerdeführers an den Rechtsanwalt der Bürgerinitiative und forderten diesen zur Löschung der Akte und der Aktenbestandteile auf. Dieser lehnte die Löschung aufgrund des Vorliegens der Ausnahme nach Art. 17 Abs. 3 Buchstabe e) Datenschutz-Grundverordnung (DS-GVO) ab. Danach ist eine Löschung nicht durchsetzbar, soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Er benötige die Daten zur Wahrnehmung der Rechte seiner Mandantin im Klageerzwingungsverfahren beziehungsweise im Beschwerdeverfahren gegen die Einstellungsverfügung der Staatsanwaltschaft nach § 170 Abs. 2 Strafprozessordnung (StPO). Weiterhin benötige er die Daten zur Geltendmachung von verwaltungsrechtlichen Ansprüchen und für die Wahrnehmung eines weiteren Mandats (Verein). Zudem würde sich die Löschung der Daten nur auf die Dokumente beschränken, in denen der Beschuldigte erwähnt würde, insoweit müsse das Löschungsersuchen seitens des Beschuldigten als betroffene Person konkretisiert werden.
Aufgrund der Erhebung und Speicherung beziehungsweise Aufbewahrung der Aktenkopie liegt eine Verarbeitung von personenbezogenen Daten nach Art. 4 Nr. 2 DS-GVO vor. Personenbezogene Daten müssen nach Art. 5 Abs. 1 Buchstabe a) DS-GVO auf rechtmäßige Weise verarbeitet werden. Nach Art. 6 Abs. 1 Satz 1 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn eine der Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO erfüllt ist.
Als Rechtsgrundlage für die Verarbeitung durch den Rechtsanwalt kam vorliegend Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht. Die Verarbeitung ist danach rechtmäßig, soweit sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Nach Prüfung des dargelegten Sachverhalts ging der TLfDI davon aus, dass aufgrund der gerichtli-

chen Feststellung, dass keine Akteneinsicht in die strafrechtlichen Ermittlungsakten hätte gewährt werden dürfen, seitens des Rechtsanwalts kein berechtigtes Interesse an der weiteren Verarbeitung der Daten aus der strafrechtlichen Ermittlungsakte bestand und die Verarbeitung daher unrechtmäßig erfolgte. Daraus würde sich nach Art. 17 Abs. 1 Buchstabe d) ein Löschungsanspruch ergeben. Dieser würde sich auch nicht nur auf die Daten der betroffenen Person beziehen, sondern auf sämtliche mittels der Akteneinsicht erlangten Daten, da die Akteneinsicht durch die Staatsanwaltschaft nicht hätte gewährt werden dürfen.
Jedoch bestand in dem Fall aufgrund der von dem Rechtsanwalt gemachten Angaben eine Ausnahme von der Löschpflicht nach Art. 17 Abs. 3 Buchstabe e) DS-GVO. Danach ist eine Löschung nicht durchsetzbar, soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Die weitere Verarbeitung unterliegt aber dann einer Zweckbindung hinsichtlich der Verwendung der Daten ausschließlich im Rahmen der Wahrnehmung des bestehenden Mandats gegenüber der Bürgerinitiative. Dies ergibt sich aus § 32f Abs. 5 StPO. Hiernach dürfen Personen, denen Akteneinsicht gewährt wurde, Akten, Dokumente, Ausdrucke oder Abschriften, die ihnen überlassen worden sind, weder ganz noch teilweise öffentlich verbreiten oder sie Dritten zu verfahrensfremden Zwecken übermitteln oder zugänglich machen. *Die erlangten personenbezogenen Daten dürfen nur zu dem Zweck. für den die Akteneinsicht gewährt wurde, verwendet werden. Für andere Zwecke dürfen die Daten nur verwendet werden, wenn dafür eine Auskunft oder Akteneinsicht gewährt werden dürfte.* Daraus ergibt sich auch, dass nur eine Verwendung im Rahmen des strafrechtlichen Verfahrens, hier das Klageerzwingungsverfahren, möglich war. Für die anderen von dem Rechtsanwalt der Bürgerinitiative genannten Zwecke könnte eine Verwendung nur erfolgen, sofern hier seitens der Bürgerinitiative ein Akteneinsichtsrecht in die Strafakten bestünde, was ausweislich des Beschlusses des Landgerichts nicht der Fall ist. In anderen Verfahren könnte insoweit die Beiziehung der staatsanwaltschaftlichen Ermittlungsakten beantragt werden. Auch die Absicht, die erlangten Daten für ein weiteres Mandat zu verwenden, war aufgrund des § 32f Abs. 5 StPO als datenschutzrechtlich unzulässig zu bewerten.
Da die Daten des Beschwerdeführers bisher nicht für andere Verfahren verwendet wurden, sprach der TLfDI gegenüber dem Rechtsan-

walt der Bürgerinitiative eine Warnung nach Art. 58 Abs. 2 Buchstabe a) DS-GVO aus. Hierbei handelt es sich um eine präventive Maßnahme. Sollte trotz der Warnung eine entsprechende Datenverarbeitung stattfinden, wäre dies in einem Bußgeldverfahren als strafschärfend zu berücksichtigen (Art. 83 Abs. 2 Buchstabe i) DS-GVO).

3.4 Videoüberwachung im Wartebereich einer Arztpraxis

Eine Videoüberwachung des Wartebereichs während der Sprechzeiten in einer Arztpraxis stellt auch ohne Speicherung der Aufnahmen in Form eines Live-Monitoring am Empfangstresen einen erheblichen Eingriff in die Rechte der betroffenen Patienten dar. Sie ist aufgrund des Überwiegens von deren Interessen als unzulässige Datenverarbeitung zu bewerten. Zudem ist daneben auch immer anhand des verfolgten Zwecks zu prüfen, ob nicht mildere Maßnahmen zum gleichen Ziel führen.

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines Patienten einer größeren Arztpraxis. Diese solle unter anderem die verschiedenen Wartebereiche der Praxis mittels Videoüberkameras überwachen. Daraufhin wurde eine Vor-Ort-Kontrolle durch den TLfDI durchgeführt. Es wurden hierbei insgesamt drei Videokameras in diversen Wartebereichen festgestellt. Es erfolgten während der Praxiszeiten Liveaufnahmen ohne Speicherung, ein sogenanntes Monitoring, am Empfangstresen; außerhalb der Praxiszeiten erfolgte eine Speicherung der Aufnahmen für 72 Stunden.
Die Zulässigkeit der durch die Arztpraxis durchgeführten Videoüberwachung wird anhand des Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) beurteilt. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Als Zwecke für die Videoüberwachung gab die Verantwortliche an, dass der Gesundheitszustand der Patienten während der Praxiszeiten überwacht werden solle, in den Nachtstunden beziehungsweise außer-

halb der Praxiszeiten sollten die Videokameras der Abwehr von Einbruchsversuchen dienen. Hierin waren grundsätzlich berechtigte Interessen zu sehen.
Im weiteren Schritt war zu prüfen, ob die Videoüberwachung für den von der Verantwortlichen genannten Zweck auch erforderlich ist. Danach muss diese geeignet sein, den verfolgten Zweck zu erreichen beziehungsweise zu fördern. Außerdem darf kein anderes, gleich wirksames milderes Mittel zur Verfügung stehen, welches weniger in die Rechte der betroffenen Personen eingreift. Hier bestanden im Rahmen der Erforderlichkeit insbesondere Bedenken hinsichtlich der Überwachung der Wartebereiche während der Praxiszeiten. Der Wartebereich der Praxis muss nicht überwacht werden, um dort sitzenden Patienten, insbesondere nach der Behandlung, rasch zu Hilfe kommen zu können. So kann diesen Patienten beispielsweise ein Druckknopf in die Hand gegeben werden, den sie im Notfall betätigen können, um Hilfe herbeizurufen (BVerwG, Urteil vom 27. März 2019, Az.: 6 C 2/18). Auch sitzen während der Sprechzeiten die meisten Patienten nicht allein im Wartezimmer, sodass bei etwaigen Notfallsituationen auch durch andere Personen Hilfe beim Empfang gerufen werden könnte. Insoweit stehen diesbezüglich mildere Mittel zur Verfügung, um diesen Zweck zu erreichen. Zudem müsste eine Mitarbeiterin oder ein Mitarbeiter am Empfang pausenlos den Bildschirm der Kameras im Blick behalten, um feststellen zu können, ob sich das Befinden von Personen so verschlechtert, dass sofort reagiert werden muss. Dies ist wohl im Empfangsbereich nicht zu erwarten, da dort die Mitarbeiterinnen und Mitarbeiter ebenfalls anderen Tätigkeiten nachgehen müssen. Insoweit scheiterte es auch an der Geeignetheit der Videoüberwachung für den genannten Zweck.
Weiterhin überwogen im vorliegenden Fall auch die schutzwürdigen Interessen der betroffenen Personen die berechtigten Interessen der Verantwortlichen im Rahmen der Überwachung der Wartebereiche während der Praxiszeiten. Es muss eine einzelfallorientierte Interessenabwägung durchgeführt werden, das heißt, es ist anhand des konkreten Sachverhalts zu beurteilen, wie gewichtig die mit der Videoüberwachung verfolgten Interessen des Verantwortlichen sind und inwieweit diese durch die Videoüberwachung tatsächlich gefördert werden. Zum anderen ist anhand des konkreten Einzelfalls zu prüfen und unter Berücksichtigung der vernünftigen Erwartungen des Betroffenen zu gewichten, inwieweit die Überwachung in schutzwürdige Inte-

ressen, Grundrechte und Grundfreiheiten eingreift und welche möglichen Folgen für Betroffene daraus resultieren können. Ob vernünftige Erwartungen bestehen, beurteilt sich danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typsicherweise akzeptiert ist oder eventuell wegen eines Beziehungszusammenhangs sogar verlangt wird oder nicht.
Der Wartebereich einer Arztpraxis stellt einen sensiblen Bereich dar. Die dort wartenden Personen haben gesundheitliche Probleme und erwarten nicht, während der Wartezeit von einer Videokamera überwacht zu werden. Dies stellt einen erheblichen Überwachungsdruck dar. Zudem handelt es sich hier auch um die Erfassung von Gesundheitsdaten der einzelnen Patienten, da gerade beabsichtigt ist, den Gesundheitszustand während der Praxiszeiten zu überwachen. Insoweit wurde seitens des TLfDI davon ausgegangen, dass die Interessen der betroffenen Patienten überwiegen.
Nach erfolgter Anhörung der Verantwortlichen im Verwaltungsverfahren wurde die Überwachung während der Praxiszeiten eingestellt. Die Überwachung außerhalb der Sprechzeiten begegnete keinem datenschutzrechtlichen Bedenken. Die verantwortliche Arztpraxis wurde jedoch durch den TLfDI hinsichtlich der bisher unzulässig während der Sprechzeiten betriebenen Videoüberwachung in den Wartebereichen nach Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt.

3.5 Ständige Kassenüberwachung in Echtzeit konform mit Beschäftigtendatenschutz?

Eine präventive dauerhafte Videoüberwachung ohne Anhaltspunkte für konkrete Straftatbestände beziehungsweise wegen des Entwendens lediglich geringer Geldbeträge stellt nach Auffassung des TLfDI eine unverhältnismäßige Verarbeitung von Beschäftigtendaten dar.

Ein Beschwerdeführer trat an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran, da er in einem Erfurter Verkaufs- und Gastronomiebetrieb von mehreren Videokameras beobachtet worden sei.
Der Verantwortliche teilte dem TLfDI im Rahmen des nachfolgend gegen ihn gerichteten Auskunftsersuchens mit, dass ausschließlich die bei ihm Beschäftigten von der Überwachung betroffen seien. Dabei erfolge keine Überwachung der gesamten Ladenfläche, sondern lediglich eine Überwachung der Kassen. Eine Überwachung von Kunden

durch die Kameras erfolge nicht. Im Rahmen des Verwaltungsverfahrens stellte sich heraus, dass Kunden tatsächlich nicht von der Überwachung berührt werden.
Als Begründung für die Kassenüberwachung der MitarbeiterInnen führte der Verantwortliche aus, es sei in der Vergangenheit zu „negativen Vorfällen und zu nicht erklärbaren Kassendifferenzen“ gekommen. Diesen sollte präventiv vorgebeugt werden und im Falle von Straftaten eine Beweissicherung erfolgen. Die festgestellten Kassendifferenzen sowie die einzelnen Straftatbestände wurden von dem Verantwortlichen im Verwaltungsverfahren lediglich allgemein erklärt.
Weiterhin ermögliche die eingesetzte Technik, nach Geschäftsschluss Bewegungen zu erkennen, was dem Einbruchsschutz in Nachtzeiten diene. Gegen diese Funktion bestanden seitens des TLfDI keine datenschutzrechtlichen Bedenken, weil nach Geschäftsschluss die Erfassung von Mitarbeitern ausgeschlossen ist, es sei denn, dass die Geschäftsräume auch nach Geschäftsschluss nochmals betreten werden müssten.
Der TLfDI untersagte nach entsprechender Anhörung des Verantwortlichen den Betrieb der Kameras. Hiergegen klagte der Verantwortliche. Erstmals im Klageverfahren gab der Verantwortliche nähere Informationen zu Zwecken der Videoüberwachung, bezifferte insbesondere die (vermeintlichen) eher geringen Kassendifferenzen und führte aus, dass Eingabefehler oder gar vorsätzliches Verhalten der Mitarbeiter hierfür schuld seien. Diese Kassendifferenzen seien Anlass für die streitgegenständliche Videoüberwachung gewesen. Derartig geringe Beträge – mögen sie auch beispielhaft genannt sein – sind nach Auffassung des TLfDI nicht geeignet, eine Videoüberwachung aller Beschäftigten zu rechtfertigen. Der Verantwortliche gab an, alle Mitarbeiter zeitlich unbefristet und anlassunabhängig zu überwachen. Damit stünden alle Beschäftigten wegen der Beobachtung unter einem dauerhaften Generalverdacht.
Eine präventive und dauerhafte Videoüberwachung aufgrund von Diebstählen lediglich geringer Geldbeträge stellt dabei vorliegend eine unverhältnismäßige Verarbeitung der Beschäftigtendaten dar und ist hier auch nicht von § 26 Abs. 1 Satz 1 und 2 Bundesdatenschutzgesetz (BDSG) gedeckt.
Die Zulässigkeit einer Videoüberwachung des Arbeitsplatzes ist nach den Kriterien von § 26 BDSG zu beurteilen. Im vorliegenden Fall dient die Datenverarbeitung nach Auffassung des TLfDI weder der

Begründung, Durchführung oder Beendigung von Beschäftigungsverhältnissen (§ 26 Abs. 1 Satz 1 BDSG). Auch eine Rechtfertigung über § 26 Abs. 1 Satz 2 BDSG scheidet aus, da diese nur dann gegeben ist, wenn aufgrund belegter konkreter Anhaltspunkte die Begehung von Straftaten durch einzelne Beschäftigte aufgedeckt werden soll. Dies hat der Verantwortliche im Klageverfahren so nicht vorgetragen.
Der Arbeitgeber muss vor der Einrichtung einer Videoüberwachung eine Datenschutzfolgenabschätzung nach Art. 35 Datenschutz-Grundverordnung (DS-GVO) durchführen sowie den/die Datenschutzbeauftragte(n) und – wenn vorhanden – den Betriebs- beziehungsweise Personalrat miteinbeziehen.
Zudem müssen alle Beschäftigten im Falle einer offenen Videoüberwachung umfassend über Zweck, Art und Umfang der Videoüberwachung sowie über ihre Rechte nach Art. 12 und 13 DS-GVO informiert werden.
Im vorliegenden Fall konnten die Kassenfehlbeträge nach Aussage des Verantwortlichen bisher nicht aufgeklärt werden. Die Videoüberwachung lieferte seit deren Inbetriebnahme also keinerlei Aufklärung von vermeintlichen Straftaten oder sonstigen Ursachen von Kassenfehlbeträgen. Die Videoüberwachung ist daher aus Sicht des TLfDI nicht geeignet, den angegebenen Überwachungszweck zu erreichen.
Um nachvollziehen zu können, ob Beschäftigte falsche Beträge in die Kasse einbuchen, müsste der gesamte Einbuchungsvorgang einschließlich der Waren des Kunden durch die Kamera erfasst werden. Da Kunden und Waren jedoch durch die Kameras nicht erfasst werden, kann auch anhand des übertragenen Erfassungsbildes nicht festgestellt werden, ob das, was der/die MitarbeiterIn gerade in die Kasse eingibt, richtig oder falsch ist.
Selbst wenn der Verantwortliche anhand der Livestream-Aufnahmen sofortige Beweissicherungsmaßnahmen einleiten wollte, setzte dies voraus, dass der Verantwortliche permanent via App auf die Aufnahmen zugreifen würde. Dann jedoch handelt es sich nicht um eine „punktuelle“ oder „minimalinvasive“ Maßnahme, wie der Verantwortliche dies darzustellen versucht, sondern um eine lückenlose Überwachung.
Der Verantwortliche gibt – wie oben berichtet – an anderer Stelle an, alle Mitarbeiter zeitlich unbefristet und anlassunabhängig zu überwachen. Das Argument der „Minimalinvasion“ geht insoweit fehl.
Neben der vorliegend fehlenden Geeignetheit der Videoüberwachung zu den angegebenen Zwecken sind im Rahmen der „Erforderlichkeit“

mildere Mittel als eine Überwachung der MitarbeiterInnen mittels Videokameras zu prüfen. Als mildere Mittel für die angegebenen Zwecke kommen dabei nicht nur stichprobenhafte Vor-Ort-Kontrollen durch den Verantwortlichen oder durch von ihm beauftragte Personen in Betracht, sondern auch Tagesinventuren oder eingeteilte Kassen für jede/n MitarbeiterIn pro Schicht mit Kassenwechsel bei Schichtwechsel.
Im Ergebnis kann die offene Videoüberwachung der Kassenbereiche, die mit einer dauerhaften Überwachung der Beschäftigten an den Kassen einhergeht, vorliegend nicht als gerechtfertigt angesehen werden. Das Klageverfahren ist noch nicht abgeschlossen. Der TLfDI wird im nächsten Tätigkeitsbericht weiter darüber berichten.

3.6 Kamera-Attrappen: Bitte Belege aufbewahren!

Kamera-Attrappen unterfallen nicht den Regelungen der DS-GVO, da sie keine Daten verarbeiten. Der Betreiber einer Attrappe ist dennoch nach Art. 5 Abs. 2 DS-GVO verpflichtet, die Funktionslosigkeit gegenüber der Aufsichtsbehörde nachzuweisen. Es empfiehlt sich deshalb, entsprechende Belege (zum Beispiel Rechnungen, Betriebsanleitungen) aufzubewahren.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat es insbesondere im Bereich der privaten Videoüberwachung immer wieder mit der Überprüfung von Videokameras zu tun, welche sich letztlich als Attrappen herausstellen. Sobald dem TLfDI ein Hinweis oder eine Beschwerde bezüglich einer vermeintlichen Videoüberwachung vorliegt, wendet er sich mit einem Auskunftsersuchen an den Verantwortlichen, um nähere Informationen über die (vermeintlichen) Kameras zu erhalten, anhand derer der TLfDI schließlich die datenschutzrechtliche Prüfung vornimmt. Oftmals erhält der TLfDI dann die Behauptung, dass es sich bei der Kamera um eine sogenannte Attrappe handele. Sofern es sich bei der Kamera tatsächlich um eine Attrappe handelt, findet keine Datenverarbeitung nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nrn. 1 und 2 Datenschutz-Grundverordnung (DS-GVO) statt. In diesem Fall wäre die DS-GVO nicht anwendbar und der TLfDI könnte mangels Zuständigkeit keine aufsichtsbehördlichen Maßnahmen erlassen.
Wendet nun der vermeintlich Verantwortliche ein, er benutze lediglich eine Kamera-Attrappe, so muss er diese Behauptung gegenüber

der Aufsichtsbehörde nachweisen können. Diese sogenannte Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO bewirkt eine Darlegungs- und Beweislastumkehr zu Lasten des Verantwortlichen, sodass nicht der Betroffene oder die Aufsichtsbehörde eine Verletzung der Vorschriften der DS-GVO nachweisen müssen, sondern der Verantwortliche deren Einhaltung (vergleiche Heberlein in Ehmann/Selmayr DS-GVO, 2. Auflage, Art. 5, Rn. 32). Die Rechenschaftspflicht führt dazu, dass der Verantwortliche die Funktionslosigkeit der Kamera hinreichend glaubhaft machen muss. Hierzu fordert der TLfDI von den Verantwortlichen entsprechende Nachweise an, welche belegen, dass es sich tatsächlich um eine Attrappe handelt (vergleiche allgemein zur Rechenschaftspflicht Heberlein in Ehmann/Selmayr, Art. 5, Rn. 32; vergleiche auch Roßnagel in Simitis/Hornung/Spiecker, Datenschutzrecht DS-GVO mit BDSG, 1. Auflage 2019, Art. 5, Rn. 186 und zur Auskunftspflicht Selmayr in Ehmann/Selmayr DS-GVO, 2. Auflage, Art. 58, Rn. 12). Denkbar sind etwa Rechnungen oder andere Kaufbelege, Hersteller-Nachweise, technische Datenblätter und Nahaufnahmen, aus denen sich ergibt, dass die Kamera nicht in der Lage ist, personenbezogene Daten zu verarbeiten. Der TLfDI fordert deshalb in solchen Fällen den Verantwortlichen auf, entsprechende Nachweise zu erbringen. Sollte dieser der Aufforderung nicht ausreichend nachkommen, ist zunächst im Einzelfall aufgrund des objektiven Erscheinungsbildes davon auszugehen, dass es sich um eine funktionsfähige Kamera handelt. Der TLfDI erlässt dann regelmäßig einen Bescheid, welcher den Verantwortlichen zur Auskunftserteilung hinsichtlich der (vermeintlichen) Kamera verpflichtet.

Es empfiehlt sich deshalb, beim Kauf einer Kamera-Attrappe diesbezügliche Belege für eine mögliche Prüfung durch die Aufsichtsbehörde aufzubewahren. Andernfalls kann der Nachweis, dass die Kamera keine Daten verarbeitet, den Verantwortlichen vor größere Probleme stellen.

Unabhängig von der Entscheidung der Aufsichtsbehörde sollte weiterhin bedacht werden, dass betroffenen Personen auch bei Attrappen die Klage vor den Zivilgerichten offensteht. Eine Attrappe, die den Verdacht einer Überwachung begründet, kann einen erheblichen Überwachungsdruck auf Personen ausüben. Diese Personen können hieraus möglicherweise zivilrechtliche Abwehransprüche (Unterlassungs- oder Schadenersatzansprüche) gegen den Nutzer der Attrappe geltend machen. Hierfür ist der TLfDI jedoch nicht zuständig.

3.7 Videoüberwachung von öffentlichen Straßen grundsätzlich unzulässig!

Eine Videoüberwachung von öffentlichen Straßen durch nicht-öffentliche Stellen ist grundsätzlich unzulässig. Sie kann nur in besonderen Ausnahmefällen nach Art. 6 Abs. 1 Buchstabe f) DS-GVO zulässig sein.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte eine Anfrage eines Thüringer Vereins erhalten, der unter anderem zum Schutz vor Diebstählen und Brandstiftungen die einzige Zufahrtsstraße zu seinem Vereinsgelände mit einer Videokamera überwachen wollte. Es bestand dabei die Möglichkeit, dass je nach Ausrichtung der Kamera verschiedene Personen in den Aufnahmebereich geraten konnten, etwa Mitarbeiter und Besucher des Vereins, Passanten und Spaziergänger sowie Eigentümer und Nutzer der anderen anliegenden, aber unbebauten Grundstücke.
Die datenschutzrechtliche Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen richtet sich zunächst nach den Vorgaben der Datenschutz-Grundverordnung (DS-GVO), da durch Kameras eine Verarbeitung von personenbezogenen Daten nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 und 2 DS-GVO vorgenommen wird. Die Verarbeitung von personenbezogenen Daten muss sich dabei an die Vorgaben in Art. 5 Abs. 1 DS-GVO halten, zu denen nach Art. 5 Abs. 1 Buchstabe a) DS-GVO der Grundsatz der Rechtmäßigkeit der Datenverarbeitung gehört. Rechtmäßig ist eine Datenverarbeitung nur unter einer der in Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO genannten Rechtsgrundlagen.
Bei der Überwachung einer öffentlichen Straße kann in der Regel allenfalls eine Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht kommen. Demnach muss die Überwachung zur Wahrung der berechtigten Interessen des für die Überwachung Verantwortlichen oder eines Dritten erforderlich sein. Die Interessen oder Grundrechte und Grundfreiheiten der von der Überwachung betroffenen Personen, die den Schutz personenbezogener Daten erfordern, dürfen dabei nicht überwiegen. Es ist bei Bejahung berechtigter Interessen des Verantwortlichen eine Interessenabwägung mit den Rechten der Betroffenen der Datenverarbeitung, also aller Personen, die in den Erfassungsbereich der Kamera geraten, vorzunehmen.

Sofern die Videoüberwachung der Vermeidung und Aufklärung von Straftaten dient, kann dies ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO darstellen, wenn dieses Schutzinteresse glaubhaft gemacht werden kann. Dies ist zu dokumentieren (Art. 5 Abs. 2 DS-GVO).
Weiterhin muss die Videoüberwachung zur Durchsetzung der berechtigten Interessen erforderlich sein (sogenannter Grundsatz der Zweckbindung nach Art. 5 Abs. 1 Buchstabe b) DS-GVO). Videoüberwachungsmaßnahmen sollten nur dann ergriffen werden, wenn der Zweck der Verarbeitung nicht durch andere Mittel erreicht werden kann, die weniger in die Grundrechte der betroffenen Person eingreifen. Je nach Fallgestaltung kann etwa bereits ein stärkeres Türschloss oder die Umzäunung des Grundstücks ausreichend sein.
Die Verarbeitung von personenbezogenen Daten muss auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“ nach Art. 5 Abs. 1 Buchstabe c) DS-GVO). Die Überwachung ist damit auf Zeiten zu begrenzen, zu denen sie wirklich notwendig ist. Vorliegend wäre dies etwa außerhalb der Öffnungszeiten des Vereins, weil die bisherigen Straftaten ausschließlich zu diesen Zeiten begangen wurden.
Im Rahmen der Interessenabwägung sind weiterhin die berechtigten Interessen des Verantwortlichen mit den Interessen und Grundrechten (Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz; Art. 6 Abs. 2 Thüringer Verfassung) der Betroffenen abzuwägen. Zu beachten ist dabei, dass bei einer anlasslosen dauerhaften Überwachung öffentlicher Straßenbereiche eine Vielzahl von Verkehrsteilnehmern und Fußgängern erfasst wird, für deren Überwachung überhaupt kein Anlass besteht und die mit einer solchen Überwachung grundsätzlich auch nicht rechnen müssen. Hierbei überwiegt regelmäßig das Interesse der Betroffenen, nicht überwacht zu werden. Entscheidend ist die Intensität des Eingriffs in die Rechte und Freiheiten des Einzelnen. Hier sind die vernünftigen Erwartungen der betroffenen Person zum Zeitpunkt der Verarbeitung ihrer personenbezogenen Daten zu berücksichtigen. Insoweit ist die Überwachung einer öffentlichen Straße problematisch, da sich dort eine unbegrenzte Anzahl an Personen aufhält, die an dieser Stelle nicht mit einer Überwachung rechnen. Grundsätzlich ist deshalb die Überwachung des öffentlichen Raumes durch nicht-öffentli-

che Stellen unzulässig (vergleiche zur Interessenabwägung BGH, Urteil vom 16. März 2010, Az. VI ZR 176/09; BGH, NJW 1995, 1955, 1957).
Vorliegend war zu Gunsten der Interessen des Verantwortlichen zu werten, dass es sich bei der zu überwachenden Straße um eine Sackgasse handelte, die kurz hinter dem Vereinsgelände endete und folglich kein Durchgangsverkehr dort stattfand. Zudem befand sich die Straße im unbebauten Gebiet, sodass neben den Mitarbeitern und Besuchern des Vereins nicht mit einem größeren Personenkreis zu rechnen war, welcher in den Aufnahmebereich der Videoüberwachung geraten würde. Hinzu kam, dass es sich um schwerwiegende Straftaten handelte, die regelmäßig und gehäuft auftraten. Nur im absoluten Ausnahmefall könnte die Überwachung einer öffentlichen Straße möglicherweise durch eine nicht-öffentliche Stelle zulässig sein (vergleiche Schaffland/Holthaus in Schaffland/Wiltfang DS-GVO Kommentar, Erich Schmidt Verlag, Art. 2, Rn. 78; Art. 6, Rn. 181g und Rn. 181 unter Verweis auf LG Duisburg, Urteil vom 17. Oktober 2016 – 3 O 381/15), etwa wenn der Eingriff in die Rechte der Betroffenen durch technische und organisatorische Maßnahmen begrenzt wird. Zu diesen Maßnahmen kann die Begrenzung folgender Faktoren gehören: Umfang der Aufnahmen beziehungsweise des Erfassungsbereichs der Kamera beispielsweise durch Verpixelung oder Schwärzung bestimmter Aufnahmebereiche (Sind Fahrer und Fußgänger zu erkennen?), Zoom- und Schwenkbarkeit der Kamera, Dauer der Überwachung, Speicherdauer der Aufnahmen. Ebenfalls könnte die Anwendung einer „Black-Box“-Lösung in Betracht kommen, bei der das Filmmaterial nach Ablauf einer bestimmten Speicherfrist automatisch gelöscht und nur im Falle eines Vorkommnisses zum Beispiel von der Polizei eingesehen wird. Der TLfDI betont, dass jede Videoüberwachung im Einzelfall auf ihre datenschutzrechtliche Zulässigkeit zu prüfen ist. Eine Überwachung öffentlicher Bereiche durch Privatpersonen bleibt grundsätzlich unzulässig.
Sollte die Videoüberwachung im Einzelfall nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zulässig sein, müsste der Verantwortliche allerdings weiterhin seinen Transparenz- und Informationspflichten nach Art. 13 DS-GVO nachkommen, indem er auf die Videoüberwachung hinweist. Hierfür müsste, für die betroffenen Personen gut sichtbar, ein entsprechendes Hinweisschild (siehe Muster auf der Internetseite des TLfDI) vor dem überwachten Bereich angebracht werden.

Es ist insgesamt anzuraten, die Überwachung, sollte sie für notwendig befunden werden, auf das eigene Grundstück zu begrenzen. Hier ist eine Interessenabwägung zu Gunsten des Verantwortlichen grundsätzlich anzunehmen oder es liegt sogar ein Fall des Art. 2 Abs. 2 Buchstabe c) DS-GVO vor („Haushaltsprivileg“ bei Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten), für den der TLfDI wegen Nichtanwendung der DS-GVO nicht zuständig wäre.

3.8 Videoüberwachung im Kuhstall

Bei der Videoüberwachung in einem landwirtschaftlichen Betrieb sind, wie in anderen Unternehmen auch, die Rechte der Beschäftigten als betroffene Personen besonders zu beachten. Der TLfDI kann hinsichtlich datenschutzrechtlicher Bestimmungen beratend tätig werden. Die Einhaltung der Regelungen der DS-GVO obliegt jedoch dem Verantwortlichen für die Videoüberwachung.

Ein landwirtschaftlicher Betrieb mit etwa 50 Mitarbeiterinnen und Mitarbeitern fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob eine von ihm testweise durchgeführte Videoüberwachung zulässig sei. Die Überwachungsanlage bestand aus mehreren Kameras, welche den Zugang zum Betriebsgelände und das Betriebsgelände selbst überwachten, insbesondere einen Kuhstall und eine Waage zur Kontrolle, wie die Traktoren beladen sind. Kühe und Traktoren liefern zwar grundsätzlich keine personenbezogenen Daten, von den Kameras konnten aber auch Mitarbeiterinnen und Mitarbeiter des Betriebs während ihrer Arbeit erfasst werden, wenn sie in deren Aufnahmebereich gerieten.
Der TLfDI ist gerne bereit, bei datenschutzrechtlichen Fragestellungen beratend tätig zu werden. Es obliegt jedoch dem Verantwortlichen für die Videoüberwachung nach Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO), also hier dem Betreiber des landwirtschaftlichen Betriebes, die Einhaltung der datenschutzrechtlichen Bestimmungen im konkreten Einzelfall zu prüfen.
Die Zulässigkeit einer Videoüberwachung durch einen landwirtschaftlichen Betrieb als nicht-öffentliche Stelle richtet sich nach den Vorgaben der DS-GVO, da durch die Kameras eine Verarbeitung von personenbezogenen Daten nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 und 2 DS-GVO vorgenommen wird. Die Verarbeitung muss

sich dabei an die Grundsätze in Art. 5 Abs. 1 DS-GVO halten, insbesondere den Grundsatz der Rechtmäßigkeit der Datenverarbeitung in Art. 5 Abs. 1 Buchstabe a) DS-GVO. Rechtmäßig ist eine Datenverarbeitung, wenn eine der in Art. 6 Abs. 1 Satz 1 Buchstaben a) bis f) DS-GVO genannten Rechtsgrundlagen erfüllt ist (siehe auch die Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen der Datenschutzkonferenz mit Stand vom 17. Juli 2020 in Ergänzung der Leitlinie 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, beides abrufbar über https://www.tlfdi.de/datenschutz/videoueberwachung/).

Werden Mitarbeiter von Kameras erfasst, muss unterschieden werden, ob der Zweck der Überwachung die Überwachung der Mitarbeiter ist – dann käme als Rechtsgrundlage § 26 Bundesdatenschutzgesetz (BDSG) in Betracht – oder ob die Mitarbeiter nicht überwacht werden sollen, aber dennoch bei der Verrichtung ihrer Tätigkeit ins Bild geraten – dann ist Art. 6 Abs. 1 Buchstabe f) DS-GVO als Rechtsgrundlage zu prüfen.

Auf § 26 Abs. 1 BDSG als Rechtsgrundlage für die Videoüberwachung konnte sich der anfragende Betrieb nicht stützen, weil die Videoüberwachung zweifellos nicht für die Durchführung oder gar Beendigung des Beschäftigungsverhältnisses erforderlich sein konnte und das Vorliegen einer Straftat durch einzelne Mitarbeiter, die eine zeitlich begrenzte Überwachungsmöglichkeit hätte ermöglichen können, nicht dargelegt worden war.

Die Zulässigkeit der Erfassung von Mitarbeitern kann auch nicht so einfach auf deren Einwilligung nach § 26 Abs. 2 BDSG gestützt werden. Eine Einwilligung muss nämlich immer freiwillig sein (Art. 7 DS-GVO). Genau das ist im Beschäftigungsverhältnis problematisch, da insbesondere aufgrund der bestehenden Abhängigkeit der Beschäftigten wegen des Über- und Unterordnungsverhältnisses zwischen Arbeitgeber und Beschäftigten regelmäßig keine Freiwilligkeit vorliegt. In den in § 26 Abs. 2 BDSG genannten Ausnahmefällen (rechtliche oder wirtschaftliche Vorteile für die Beschäftigten oder gleichgelagerte Interessen mit dem Arbeitgeber) kann von einer freiwillig erteilten Einwilligung ausgegangen werden.

Im vorliegenden Fall kam daher als Rechtfertigungsgrund nur Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht. Nach dieser Norm bedarf es zur Zulässigkeit der Datenverarbeitung zunächst eines berechtigten Interesses des Verantwortlichen oder eines Dritten, wobei

die Datenverarbeitung zur Erfüllung dieses berechtigten Interesses erforderlich sein muss. Die Interessen oder Grundrechte und Grundfreiheiten von betroffenen Personen, die den Schutz personenbezogener Daten erfordern, dürfen dabei nicht überwiegen. Dabei ist das starke Interesse der Beschäftigten, nicht überwacht zu werden, mit den Interessen des Betriebs abzuwägen. Der Verantwortliche muss für jede von ihm eingesetzte Videokamera einen konkreten Zweck für die Überwachungsmaßnahme festlegen. Berechtigte Interessen eines Verantwortlichen können rechtliche, wirtschaftliche oder immaterielle Interessen sein, sofern sie tatsächlich und aktuell bestehen, also nicht nur fiktiv oder spekulativ sind. Der landwirtschaftliche Betrieb gab an, die Überwachung zur Sicherung des Betriebsgeländes vor einem unbefugten Zutritt, zur Kontrolle des Stalls, insbesondere dem Verschluss der Tiere und der Sichtung der Fahrzeugwaage zu nutzen.
Weiterhin muss die geplante Überwachung zur Erreichung des legitimen Zweckes erforderlich, also angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“ nach Art. 5 Abs. 1 Buchstabe c) DS-GVO). Videoüberwachungsmaßnahmen sollten nur dann gewählt werden, wenn der Zweck der Verarbeitung nach vernünftigem Ermessen nicht durch andere Mittel erreicht werden kann, die weniger in die Grundrechte und Grundfreiheiten der betroffenen Person eingreifen („mildere Mittel“).
Im vorliegenden Fall musste insbesondere eine dauerhafte Videoüberwachung hinterfragt werden. Gemessen am Zweck der Überwachung war zu prüfen, ob das anlassbezogene Aktivieren der Kameras, etwa nur beim Betrieb der Waage oder wenn keine Beschäftigten vor Ort sind, um die Türen zum Stall oder das Gelände zu kontrollieren, als milderes Mittel ausreichend und ob eine Speicherung der Aufnahmen notwendig ist. Möglicherweise ist bereits eine Echtzeitübertragung auf einen Monitor ohne Speicherung der Aufnahmen durch „Live-Monitoring“ ausreichend.
Sofern der Schutz des Eigentums und bestehende Sicherheitsinteressen als Zweck der Überwachung angeführt werden, ist zu überprüfen, ob nicht andere Maßnahmen in gleicher Weise geeignet sind. So wies der TLfDI im vorliegenden Fall den verantwortlichen Betrieb darauf hin zu prüfen, ob gegebenenfalls der Einsatz von Sicherheitspersonal zur Kontrolle des Zugangs zum Betriebsgelände ausreichend sein könnte.

Im Rahmen der vorzunehmenden Interessenabwägung müssen die betrieblichen (Sicherheits-)Interessen des Verantwortlichen die Interessen und Grundrechte (Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) der Betroffenen, hier der Beschäftigten, überwiegen. Entscheidend ist die Intensität des Eingriffs in die Rechte und Freiheiten des Einzelnen. Hier sind die vernünftigen Erwartungen der betroffenen Person zum Zeitpunkt der Verarbeitung ihrer personenbezogenen Daten zu berücksichtigen. So muss ein Beschäftigter an seinem Arbeitsplatz in den meisten Fällen nicht damit rechnen, dass alle seine Tätigkeiten und Bewegungen von seinem Arbeitgeber überwacht werden.
Beschäftigte dürfen nicht einem ständigen Überwachungs- und Beobachtungsdruck und der Möglichkeit einer vollständigen Leistungs- und Verhaltenskontrolle ausgesetzt werden. Um dies zu verhindern, könnten etwa die Kameras nur außerhalb der Betriebszeiten aktiviert werden, soweit dies den Zweck der Überwachung nicht gefährdet oder keine anderen milderen Mittel eingesetzt werden können. Denkbar wäre etwa die Verpixelung von Bereichen, die von Beschäftigten betreten werden. Soweit Beschäftigte oder andere sich befugt auf dem Gelände befindliche Personen dennoch erfasst werden, könnte die Anwendung einer „Black-Box“-Lösung, bei der das Filmmaterial nach Ablauf einer bestimmten Speicherfrist automatisch gelöscht und nur im Falle eines Vorkommnisses zum Beispiel von der Polizei eingesehen wird, in Betracht kommen.
Um den Anforderungen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO nachzukommen, müsste der Verantwortliche vorab, das heißt vor Inbetriebnahme der Kameras ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu jeder Kamera anlegen und gegebenenfalls eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchführen. Es ist hierin insbesondere der jeweilige Zweck der Überwachung schriftlich festzuhalten.
Sollte die Videoüberwachung hiernach zulässig sein, muss der verantwortliche Betrieb außerdem seinen Transparenz- und Informationspflichten nach Art. 13 DS-GVO nachkommen, indem er auf die Videoüberwachung hinweist. Der TLfDI hat hierzu Muster für Hinweisschilder auf seiner Website veröffentlicht, abrufbar unter:

- https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/video/anlage1_hinweisschild_final.pdf (vorgelagertes Hinweisschild)

- https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/video/anlage2_vollst_information_final.pdf (vollständiges Informationsblatt).

3.9 Pflichtfelder in einem Internetkontaktformular

Der Grundsatz der sparsamen Datenverarbeitung oder auch Grundsatz der „Datenminimierung“ besagt, dass nur personenbezogene Daten von betroffenen Personen verarbeitet werden dürfen, die für den konkreten Zweck angemessen und erforderlich sind (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Die Koppelung der Telefonnummer und der E-Mail-Adresse als Pflichtfelder in einem Internetkontaktformular ist zu begründen. Werden die Kontaktdaten für getrennte Verarbeitungszwecke benötigt, ist dies transparent auszuführen. Auch ist dann eine Einwilligung für jeden Verarbeitungszweck einzuholen (Art. 5 Abs. 1 Buchstabe a) in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO).

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten mehrere Beschwerden bezüglich Internetseiten, auf denen im Kontaktformular zur Zusendung von Anmeldeunterlagen oder Informationsmaterial zwingend die Telefonnummer sowie die E-Mail-Adresse angegeben werden mussten. So kam es vor, dass nach dem Absenden eines Kontaktformulars eine unerwünschte, telefonische Kontaktaufnahme zum Absender erfolgte. Wobei der Anruf einem anderen Zweck diente als die ursprünglich erteilte Einwilligung in die Verarbeitung der Daten, nämlich der Übersendung von Informationsmaterial.
In den Fällen kamen gleich mehrere Verletzungen gegen wichtige Datenschutzgrundsätze in Betracht. Nach dem Grundsatz der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 Buchstabe a) in Verbindung mit Art. 6 Abs. 1 Datenschutz-Grundverordnung [DS-GVO]) bedarf jede Datenverarbeitung einer Rechtsgrundlage. Bei dem Zweck des Zusendens von Informationsmaterial muss die Frage gestellt werden, was es hierfür an Daten seitens des Anfragenden braucht. In der Regel genügen hier Anrede, Name, Vorname und Post- oder E-Mail-Adresse.
Die Angabe einer Telefonnummer ist bereits grundsätzlich nicht geeignet, um Informations- oder Anmeldematerial zu übersenden. Hierzu genügt die Angabe einer E-Mail- oder Postadresse. Diese kön-

nen bei Einwilligung der Betroffenen genutzt werden, um das angeforderte Material zuzusenden. Die zusätzliche Abfrage einer Telefonnummer bedürfte ebenfalls der Einholung einer expliziten Einwilligung, wobei der Verantwortliche vorab klarstellen muss, wozu er die Telefonnummer verwenden möchte. Das war auf der Seite nicht der Fall. Somit ist ein Verstoß gegen eine sparsame Datenverarbeitung gemäß Art. 5 Abs. 1 Buchstabe c) DS-GVO seitens des TLfDI zu prüfen. Die Verantwortliche wurde hierzu nochmals angehört.
In den vorliegenden Prüfverfahren ergab sich zudem ein Verstoß gegen den Grundsatz der transparenten Datenverarbeitung (Art. 5 Abs. 1 Buchstabe a) DS-GVO). In den Datenschutzhinweisen auf der Webseite der Verantwortlichen wurden keine Informationen darüber bereitgehalten, wofür die Verantwortliche der Webseite die Telefonnummer benötigte und schließlich verwendete.
Da die Verantwortliche die Telefonnummer für Anrufe zum Erreichen eines anderen Zweckes nutzte, hier dem Abschluss eines Vertrages, hätte sie die betroffene Person über diesen anderen Zweck informieren müssen. Das bloße Anfordern von Anmeldeunterlagen oder Informationsmaterial setzt nicht zwingend einen sich anschließenden Vertragsabschluss voraus. Somit diente die Telefonnummer nicht der Zusendung des angeforderten Materials an sich, sondern eher dem Zweck einer Werbemaßnahme. Dies muss als solche auch kenntlich gemacht werden. Die Nutzer sind bei der Einholung der Einwilligung im Kontaktformular darauf hinzuweisen, dass die Verantwortliche die Telefonnummer für spätere Anrufe nutzen darf.
Die Verwaltungsverfahren sind noch nicht alle abgeschlossen. Der Thüringer Landesbeauftragte wird im nächsten Tätigkeitsbericht weiter berichten.

3.10 Aktenzeichen XY ungelöst: Die Patientenakte bleibt verschwunden

Wenn ein Patient gemäß Art. 7 Abs. 1 DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO seine Einwilligung dazu erteilt, dass seine Patientenakte an einen neuen, den Patienten weiterbehandelnden Arzt geschickt werden soll, so ist der Verantwortliche (bisheriger Arzt) gehalten, die Patientenakte zu übersenden. Der Verlust einer Patientenakte stellt nach Art. 5 Abs. 1 Buchstabe f) DS-GVO eine Verletzung des Schutzes personenbezogener Daten dar und ist nach Art. 33 DS-GVO der Aufsichtsbehörde zu melden.

Im Februar 2022 beschwerte sich ein Patient beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Poliklinik in Südthüringen. Der Betroffene hatte die Klinik bereits im März 2021 gebeten, die über ihn verarbeiteten, personenbezogenen Gesundheitsdaten (Patientenakte) seiner ehemaligen Hausärztin an seine neue Hausarztpraxis zu übersenden. Jedoch waren seine Unterlagen von der Klinik bis Februar 2022 nicht übersandt worden. Auf seine wiederholte Aufforderung zur Übersendung der Unterlagen teilte die Klinik dem Betroffenen im Januar 2022 mit, dass die „Altakten" seiner ehemaligen Hausärztin dezentral archiviert würden und die Klinik den Archivierungsdienstleister beauftragt habe, sämtliche Akten der Hausärztin an die Klinik zu übersenden, um die Akte des Betroffenen herauszusuchen; dies könne jedoch vier Wochen dauern. Das Ersuchen des Patienten erstreckte sich ausschließlich auf Patientenakten seiner ehemaligen Hausärztin, die von der Klinik lediglich verwahrt wurden und nicht auf aktuelle Behandlungsakten des Patienten aus dem Klinikum.

Der TLfDI wandte sich aufgrund der Beschwerde des Patienten an das Klinikum und forderte Auskunft von der Klinik, welche Gründe der Übersendung der vom Beschwerdeführer angeforderten personenbezogenen Daten (Patientenakte) an seine neue Hausärztin entgegenstehen und aus welchem Grunde die Klinik die Altakten der ehemaligen Hausärztin des Beschwerdeführers nicht bereits nach dessen Anforderung und Einwilligung im März 2021 vom externen Archivierungsdienstleiter angefordert hatte.

Daraufhin teilte die Klinik mit, dass die Patientenakte des Beschwerdeführers nicht auffindbar sei und sie den Beschwerdeführer darüber informieren wolle, dass seine Patientenakte im Rahmen der Archivierung verloren gegangen sei. Der TLfDI wies die Klinik darauf hin, dass der Verlust einer Patientenakte eine Verletzung des Schutzes personenbezogener Daten nach Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) darstellt und dies nach Art. 33 Abs. 1 DS-GVO der Aufsichtsbehörde zu melden ist. Wenn ein Verantwortlicher seiner Meldepflicht nach Art. 33 Abs. 1 DS-GVO nicht nachkommt, kann er sich hinsichtlich der Erhebung eines Bußgeldes wegen Verstoßes gegen die Vorgaben der DS-GVO auch nicht auf § 43 Abs. 4 Bundesdatenschutzgesetz berufen. Somit ist die Verhängung eines Bußgeldes wegen eines festgestellten Verstoßes grundsätzlich möglich. Im vorliegenden Fall war die Meldung des Verlustes der Pa-

tientenakte gemäß Art. 33 Abs. 1 DS-GVO entbehrlich, da die Information dem TLfDI im Zuge der Beschwerde zeitgleich mit der Kenntnis der Klinik vorlag. Da bei einem Verlust von Gesundheitsdaten, vorliegend einer gesamten Patientenakte, voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen besteht, ist der Beschwerdeführer nach den Vorgaben des Art. 34 Abs. 1 DS-GVO über den Verlust seiner Patientenakte durch die Klinik zu informieren. Der TLfDI teilte der Klinik mit, dass er im Falle einer unterbleibenden Information des Betroffenen die unverzügliche Benachrichtigung des Betroffenen über den Verlust seiner Patientenakte nach Art. 34 Abs. 4 DS-GVO in Verbindung mit Art. 58 Abs. 2 Buchstabe e) DS-GVO anordnen wird.
Weiterhin wies der TLfDI die Klinik auf ihre Verpflichtung gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 Buchstabe c) DS-GVO hin, bei Feststellung des Verlustes von personenbezogenen Daten zu prüfen, ob es möglich ist, die Daten wiederherzustellen oder ob Ersatzdokumente zur Verfügung stehen. Im Regelfall werden Patientenakten vom behandelnden Arzt auch elektronisch geführt. Der TLfDI teilte der Klinik mit, dass er eine entsprechende Prüfung nach Art. 58 Abs. 2 Buchstabe d) DS-GVO anordnen werde, sofern die Klinik diesen Sachverhalt nicht bereits geprüft hat. Daraufhin teilte die Klinik Ende April 2022 mit, dass die Patientenakte des Beschwerdeführers nicht mehr rekonstruiert werden könne, da sie nur in Papierform geführt wurde und dass die Klinik den Betroffenen bereits schriftlich über den Verlust seiner Patientenakte gemäß Art. 34 Abs. 1 DS-GVO informiert habe.
Es war nicht mehr rekonstruierbar, an welcher Stelle und zu welchem Zeitpunkt die Akte des Beschwerdeführers verlorengegangen ist. Hierfür kamen mehrere, nicht nachprüfbare Möglichkeiten in Betracht. So konnte die Verantwortung für die verschwundene Akte auch bei der ursprünglichen Ärztin liegen, die die Akten zur Verwahrung an die Klinik gegeben hatte – die Akte konnte bereits bei der Ärztin selbst oder beim Übergang der Akte von der Ärztin zur Klinik verschwunden gewesen sein. Sie konnte aber auch auf dem Transport zum Archivierungsunternehmen beziehungsweise vom Archivierungsunternehmen zur Klinik verloren gegangen sein. Die Klinik hatte keine weiteren Unterlagen, da sie die Patientenakten nur verwahrt hatte und nicht selbst Behandler gewesen war. Somit war der Verantwortliche für den Verlust der Akte nicht eindeutig ermittelbar und die Angelegenheit datenschutzrechtlich nicht weiter prüfbar.

Der TLfDI informierte den Beschwerdeführer darüber, dass es sich bei dem Verlust seiner personenbezogenen Gesundheitsdaten (Patientenakte) um eine Verletzung des Schutzes personenbezogener Daten handelte, aufgrund der Umstände jedoch nicht mehr rekonstruierbar ist, an welcher Stelle und zu welchem Zeitpunkt seine Patientenakte verlorengegangen war, da hierfür mehrere, nicht nachprüfbare Möglichkeiten in Betracht kamen. Der TLfDI legte dem Beschwerdeführer die in Frage kommenden Möglichkeiten für den Verlust seiner Patientenakte dar und teilte ihm mit, dass der Verantwortliche für den Verlust datenschutzrechtlich nicht eindeutig ermittelbar ist und der TLfDI die Angelegenheit datenschutzrechtlich somit nicht weiterverfolgen kann.

3.11 Für Wertsachen wird keine Haftung übernommen – das gilt auch für die eigenen personenbezogenen Daten

Wenn der Verantwortliche alle technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ergreift, die zum Schutz von personenbezogenen Daten erforderlich sind, kann es ihm datenschutzrechtlich nicht angelastet werden, wenn die betroffene Person selbst ihre personenbezogenen Daten in den Räumlichkeiten des Verantwortlichen unbefugten Dritten zugänglich macht. In diesem Fall liegt keine Verletzung von Integrität und Vertraulichkeit personenbezogener Daten im Sinne von Art. 5 Abs. 1 Buchstabe f) DS-GVO vor und eine Meldung über eine Verletzung des Schutzes von personenbezogenen Daten nach Art. 33 Abs. 1 DS-GVO muss somit auch nicht erfolgen.

Im Juni 2022 wandte sich der Datenschutzbeauftragte einer radiologischen Arztpraxis an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob die Arztpraxis auch dafür verantwortlich sei, wenn Patienten in den Räumlichkeiten der Praxis ihre personenbezogenen Gesundheitsdaten liegenlassen und somit selbst unbefugten dritten Personen zugänglich machen. Eine Patientin hatte ihre medizinischen Vorbefunde für die Röntgenuntersuchung in der abschließbaren Umkleidekabine zwischen Röntgenraum und Wartezimmer liegengelassen. Eine nachfolgende Patientin hatte die Befunde in der Umkleidekabine vorgefunden.

Die radiologische Arztpraxis verfügte über eine gesonderte Umkleidekabine zwischen Wartezimmer und Röntgenraum. Die Umkleidekabine war von innen zum Wartezimmer hin abschließbar. In der Umkleidekabine legte die Patientin vor dem Betreten des Röntgenraumes ihre Kleidung einschließlich metallischer Gegenstände und sonstiger Wertsachen ab. Für diese patienteneigenen Sachen wird seitens der Arztpraxis als Verantwortlichem keine Haftung übernommen. Darauf wurde auch durch ein entsprechendes Schild in der Umkleidekabine hingewiesen. Die betroffene Patientin vergaß nach dem Ankleiden und Verlassen der Umkleidekabine jedoch ihre medizinischen Befunde in der Kabine, sodass diese dort liegenblieben. Eine nachfolgende Patientin nahm die Befunde versehentlich mit. Die Tochter der nachfolgenden Patientin entdeckte den Irrtum und übergab die Befundunterlagen der radiologischen Praxis.
Der TLfDI teilte dem Datenschutzbeauftragten der radiologischen Arztpraxis mit, dass in dem geschilderten Fall die betroffene Patientin ihre personenbezogenen Gesundheitsdaten aufgrund des Liegenlassens in der Umkleidekabine selbst unbefugten dritten Personen im Sinne von Art. 4 Nr. 10 Datenschutz-Grundverordnung (DS-GVO), vorliegend der nachfolgenden Patientin, zugänglich gemacht hat. Diese Verletzung des Schutzes personenbezogener Daten kann nicht dem Inhaber der radiologischen Praxis angelastet werden.
Die Abschließbarkeit der Umkleidekabine garantiert gemäß Art. 32 Abs. 1 DS-GVO die organisatorische Sicherstellung, dass personenbezogene (Gesundheits-)Daten nicht von unbefugten Dritten entwendet werden können. Sofern die betroffene Person ihre eigenen Daten nicht selbst angemessen sichert, indem sie diese nach Ablegen in der Kabine vor der Röntgenuntersuchung und nach der Röntgenuntersuchung beim Verlassen der Kabine wieder mitnimmt, kann eine daraus resultierende Verletzung des Schutzes personenbezogener Daten aufgrund der Kenntnisnahme durch nachfolgende Patienten als unbefugte Dritte nicht dem Inhaber der radiologischen Praxis angelastet werden. Eine Meldung nach Art. 33 Abs. 1 DS-GVO war somit nicht erforderlich.

3.12 Nutzung einer Dashcam im geparkten Auto

Das Filmen von Passanten mit einer Dashcam im Auto ist grundsätzlich unzulässig, insbesondere wenn das Auto geparkt ist. Der TLfDI

kann jedoch nur aufsichtsbehördliche Maßnahmen nach Art. 58 Abs. 2 DS-GVO gegen den Verantwortlichen erlassen, wenn diesem Verstöße gegen datenschutzrechtliche Bestimmungen nachgewiesen werden können.

Ein besorgter Bürger reichte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde nach Art. 77 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ein, weil er befürchtete, von seinem Nachbarn entgegen datenschutzrechtlicher Bestimmungen überwacht worden zu sein. Der Nachbar habe in seinem Auto eine sogenannte Dashcam angebracht, welche sich bei Bewegung aktivere und sodann Aufnahmen von vorbeilaufenden Passanten und dem öffentlichen Verkehrsraum anfertige. Zudem sei das Auto überwiegend so geparkt, dass das Grundstück des Beschwerdeführers in den Aufnahmebereich der Kamera gerate.

Dashcams beziehungsweise Unfallkameras sind kleine Videokameras, die an einem Kraftfahrzeug oder Fahrrad befestigt sind und aus der Perspektive des Fahrers das Verkehrsgeschehen filmen. Die Verwendung einer Dashcam ist grundsätzlich geeignet, im Rahmen der gemachten Videoaufnahmen personenbezogene Daten von Passanten oder Verkehrsteilnehmern zu verarbeiten, weshalb die DS-GVO nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 und 2 DS-GVO Anwendung findet und ihre Regelungen zu beachten sind. Die Verarbeitung muss sich dabei an die Grundsätze in Art. 5 Abs. 1 DS-GVO halten, insbesondere den Grundsatz der Rechtmäßigkeit der Datenverarbeitung in Art. 5 Abs. 1 Buchstabe a) DS-GVO. Rechtmäßig ist eine Datenverarbeitung unter einer der in Art. 6 Abs. 1 Satz 1 Buchstaben a) bis f) DS-GVO genannten Rechtsgrundlagen.

Bei der Nutzung von Dashcams durch private Personen kommt allenfalls die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern. Die Interessen des Verantwortlichen, der eine Dashcam einsetzt, und die Interessen der davon betroffenen Personen sind gegeneinander abzuwägen. Eine entscheidende Rolle spielt dabei der Einsatzweck. Dieser muss vom Verantwortlichen eindeutig festgelegt werden, bevor er

die Aufnahmen anfertigt. In den meisten Fällen dürfte dies die Sicherung von Beweisen im Fall eines Unfalls für die spätere Schadensregulierung sein. Doch ist die konkrete Datenverarbeitung, nämlich das Filmen, auch erforderlich, um den Zweck einer Beweissicherung bei Unfällen zu erreichen? Nein. Regelmäßig ist beim Einsatz von Dashcams die Erforderlichkeit der Datenverarbeitung nicht gegeben. Diese zeichnen nämlich in aller Regel weit mehr als einen Unfall auf. Videoüberwachungsmaßnahmen sollten dabei nur dann ergriffen werden, wenn der Zweck der Verarbeitung nicht durch andere Mittel erreicht werden kann, die weniger in die Grundrechte der betroffenen Person eingreifen. Unzulässig ist jedenfalls eine permanente und anlasslose Aufzeichnung des Verkehrsgeschehens (vergleiche BGH, Entscheidung vom 15. Mai 2018 – VI ZR 233/17). Eine Ausnahme kann nur in Betracht kommen, wenn technische Vorkehrungen ergriffen werden, die sicherstellen, dass eine Kamera lediglich kurzzeitig und anlassbezogen aufzeichnet.

Zudem scheitert die anlasslose und dauerhafte Überwachung des Verkehrsraums an der nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO durchzuführenden Interessenabwägung. Die Interessen und Grundrechte (Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz; Art. 6 Abs. 2 Thüringer Verfassung) der Betroffenen überwiegen dabei ein mögliches Beweissicherungsinteresse des Verantwortlichen. Durch eine dauerhafte Überwachung öffentlicher Straßenbereiche wird eine Vielzahl von Verkehrsteilnehmern und Fußgängern erfasst, für deren Überwachung kein Anlass besteht und die mit einer Überwachung nicht rechnen müssen. Dies stellt einen nicht zu rechtfertigenden Eingriff in das Recht auf Schutz der personenbezogenen Daten der Betroffenen dar.

Eine Überwachung des öffentlichen Raumes aus einem geparkten Fahrzeug heraus, wie vorliegend vom Beschwerdeführer behauptet, ist unzulässig (vergleiche AG München, Urteil vom 9. August 2017 – 1112 OWi 300 Js 121012/17).

Zudem muss auch bei einer Videoüberwachung mittels Dashcam der Verantwortliche sicherstellen, dass er die betroffenen Personen gemäß Art. 12, 13 DS-GVO auf die Datenverarbeitung hinweist. Es erscheint realitätsfern, dass der Betreiber einer Dashcam jeden potentiellen Betroffenen vor Betreten des Erfassungsbereiches der Dashcam über die Datenverarbeitung informiert. Dies würde theoretisch voraussetzen,

dass der Verantwortliche an seinem Fahrzeug gut sichtbare Informationsblätter für die Passanten bereithält – solche Warnschilder kennt man allenfalls in Form von Piktogrammen an Lkw. Die Ausführungen des Beschwerdeführers im konkreten Fall ließen hier keine solchen Informationen des Verantwortlichen erkennen. Somit wäre die Überwachung, wie sie der Beschwerdeführer beschreibt, als unzulässig anzusehen.
Im vorliegenden Verfahren berief sich der Verantwortliche auf sein Auskunftsverweigerungsrecht nach § 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz und machte keine weiteren Angaben zum Sachverhalt. Auch ein Amtshilfeersuchen nach § 5 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz bei der zuständigen Gemeinde zur Kontrolle der Lage vor Ort führte zu keinen weiteren Erkenntnissen. Auf Nachfrage beim Beschwerdeführer erklärte dieser gegenüber dem TLfDI, der Verantwortliche besitze mittlerweile ein neues Auto und es sei nicht bekannt, ob weiterhin eine Überwachung stattfinde. Nachweise für die vormalige Nutzung einer Dashcam lagen dem Beschwerdeführer nicht vor. Damit konnte der TLfDI dem Verantwortlichen weder den Einsatz einer Dashcam noch einen Verstoß gegen datenschutzrechtliche Bestimmungen nachweisen. Im Ergebnis musste das TLfDI die Beschwerde somit nach Art. 77 Abs. 2 DS-GVO abweisen. Sollten jedoch dem Beschwerdeführer zu einem späteren Zeitpunkt Hinweise vorliegen, die auf eine Videoüberwachung durch den Verantwortlichen hindeuten, kann erneut Beschwerde beim TLfDI erhoben werden. Der TLfDI wird sodann ein neues Prüfverfahren veranlassen.
Weitere Informationen zum Einsatz von Dashcams werden von der Datenschutzkonferenz in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ vom 17. Juli 2020, hier Seite 32, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf, und dem „Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen“ vom 28. Januar 2019, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190128_oh_positionspapier_dashcam.pdf, bereitgestellt.

4. Entschließungen und Beschlüsse

Konferenz Erde Welt - Kostenloses Bild auf Pixabay - Pixabay

4.1 Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 23. März 2022

In den vergangenen Jahren gab es zahlreiche Parlamentarische Untersuchungsausschüsse im Bundestag und in den Landtagen, die das Handeln von Polizei- und Sicherheitsbehörden untersucht haben. Prominente Beispiele sind die Untersuchungsausschüsse zur „Terrorgruppe nationalsozialistischer Untergrund“ (sog. NSU).
Die Untersuchungsausschüsse möchten eine für die Aufklärung notwendige Datengrundlage sicherstellen. Deshalb fordern sie die Behörden regelmäßig auf, sämtliche personenbezogenen Daten weiterhin zu speichern, die in irgendeinem Bezug zum Untersuchungsgegenstand stehen können (etwa zum Thema „Rechtsextremismus“). Diese Daten sind dann für die Arbeit des Untersuchungsausschusses vorzuhalten.

Dies soll auch solche Daten umfassen, die nach den gesetzlichen Regeln eigentlich zu löschen wären (so genanntes Löschmoratorium).
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält das Interesse der Parlamentarischen Untersuchungsausschüsse an dem Erhalt personenbezogener Daten für nachvollziehbar und gewichtig, um den Untersuchungsauftrag umzusetzen. Es ist ihr insbesondere bewusst, dass dem parlamentarischen Informationsinteresse ein besonders hohes Gewicht zukommt, soweit es um die Aufdeckung möglicher Rechtsverstöße und vergleichbarer Missstände geht. Gleichzeitig gilt es allerdings zu berücksichtigen, dass dadurch erheblich in Grundrechte der betroffenen Personen eingegriffen wird, insbesondere dann, wenn diese Personen tatsächlich in keinerlei Bezug zum Untersuchungsgegenstand stehen bzw. gesetzliche Löschungsverpflichtungen suspendiert werden.
Um parlamentarischen Kontrollrechten und Grundrechten betroffener Personen gleichermaßen Geltung zu verschaffen, weist die Konferenz auf folgende Punkte hin:

- Ohne die förmliche Einsetzung eines Untersuchungsausschusses und Anforderungen von Beweisunterlagen gibt es keine Rechtsgrundlage dafür, die gesetzlich vorgeschriebene Löschung personenbezogener Daten zu suspendieren.
  Hierzu gehört, dass der Untersuchungsgegenstand klar definiert ist und die Beweisbeschlüsse hinreichend bestimmt formuliert sind (BVerfG, Beschluss vom 17.6.2009 – 2 BvE 3/07). Zudem müssen die Ausnahmen zeitlich auf die Arbeit des Untersuchungsausschusses begrenzt sein. Nur auf diese Weise können unnötige Datenspeicherungen und die damit verbundenen Risiken für die Rechte der betroffenen Personen vermieden werden.
- „Löschreife“ Daten, die die Behörden für Zwecke eines Untersuchungsausschusses zur Verfügung halten, dürfen sie im weiteren Verwaltungsvollzug nicht nutzen. Die DSK hält es daher für erforderlich, diese Daten in Anlehnung an § 58 Abs. 3 BDSG in ihrer Verarbeitung zu beschränken. Hierfür sollte der jeweilige Gesetzgeber Voraussetzungen und Grenzen präzise beschreiben. Einige Landesgesetzgeber haben dies bereits umgesetzt.

Die DSK appelliert deshalb an die Gesetzgeber des Bundes und der Länder, den Sicherheitsbehörden klare gesetzliche Vorgaben zum Umgang mit zu löschenden Daten zu machen. Diese müssen den Untersuchungsausschüssen den Zugriff auf die Daten sichern. Gleichzei-

tig ist sicherzustellen, dass die Daten dem Verwaltungsvollzug der Behörden entzogen sind. So werden das Untersuchungsinteresse der Parlamentarischen Untersuchungsausschüsse und die Grundrechte der betroffenen Personen gewahrt.

4.2 Wissenschaftliche Forschung – selbstverständlich mit Datenschutz

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 23. März 2022

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unterstreicht, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind.
Auch der europäische Verordnungsgeber hat die Bedeutung der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung gesehen. So privilegiert die Datenschutz-Grundverordnung (DSGVO) die wissenschaftliche Forschung an vielen Stellen. Dazu gehört beispielsweise die Regelung in Artikel 5 Absatz 1 lit. b DSGVO, wonach Forschungszwecke vereinbar mit dem ursprünglichen Zweck sein können, zu dem die Daten einmal erhoben wurden.
Dies entspricht dem politischen Ziel der Europäischen Union, den wissenschaftlichen Fortschritt zu fördern sowie ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Forschungsraum geschaffen wird.
Die DSGVO zielt daher darauf ab, einen Ausgleich zwischen der Forschungsfreiheit auf der einen Seite und dem Recht des Einzelnen auf Achtung seines Grundrechts auf Datenschutz zu schaffen. So weist Artikel 89 DSGVO darauf hin, dass Verarbeitungen von personenbezogenen Daten für die wissenschaftliche Forschung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne der DSGVO unterliegen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet werden muss. Die DSK unterstützt daher nachdrücklich die Förderung und Erforschung von Methoden, Forschungsdaten so zu verarbeiten, dass Persönlichkeitsrechte der Bürgerinnen und Bürger bestmöglich geschützt werden. Soweit ein Zugriff auf identifizierende Angaben nicht durch

geeignete innovative Methoden ausgeschlossen werden kann, sollten Anonymisierung, Pseudonymisierung, Datentreuhänderschaften und andere Instrumente vorgesehen werden.
Die DSK begrüßt die Überlegungen der Bundesregierung, ein allgemeines Forschungsdatengesetz auf den Weg zu bringen, das das Recht auf informationelle Selbstbestimmung wahrt. Flankiert werden sollte dieses allgemeine Forschungsdatengesetz durch Forschungsregelungen in einzelnen Bereichen. Insbesondere erkennt die DSK die Pläne der Bundesregierung an, ein datenschutzgerechtes Gesundheitsdatennutzungsgesetz auf den Weg zu bringen, um die Besonderheiten bei der wissenschaftlichen Forschung mit Gesundheitsdaten zu berücksichtigen. Die Erschließung von Gesundheitsdaten in medizinischen Registern für die wissenschaftliche Forschung durch ein geplantes Registergesetz kann allerdings nur unter Beachtung der datenschutzrechtlichen Anforderungen erfolgen.
Insoweit weist die DSK vor allem auf ihre Entschließung vom 25./26. März 2004[1] hin und fordert den Gesetzgeber auf sicherzustellen, dass auch bei und nach der Übermittlung geschützter personenbezogener medizinischer Daten ein strafrechtlicher Schutz vor Offenbarung und Beschlagnahmeschutz im Strafverfahren gewährleistet ist.
Aus diesem Grund hält sie es insbesondere für erforderlich,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forschende und ihre Berufshelfenden zu schaffen und
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die DSK bietet eine konstruktive Beratung bei der Weiterentwicklung der Nationalen Forschungsdateninfrastruktur an, sofern dabei personenbezogene Daten betroffen sind. Dies gilt auch im europäischen Kontext, soweit etwa im Bereich des Europäischen Gesundheitsdatenraums personenbezogene Daten, insbesondere Gesundheitsdaten, für die wissenschaftliche Forschung bereitgestellt werden sollen.
Die DSK beabsichtigt zeitnah weitere Vorschläge zum Thema Forschungsdaten zu veröffentlichen. Ziel ist es, neben der Rechtsklarheit

[1] vgl. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/67DSK-EinfuehrungEinesForschungsgeheimnissesFuerMedizinischeDaten.pdf

für die Nutzung von Forschungsdaten insbesondere auch den nachhaltigen Schutz für die personenbezogenen Daten der Bürgerinnen und Bürger zu gewährleisten.

4.3 Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt“!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 29. April 2022

Die voranschreitende technische Entwicklung ermöglicht eine immer weitergehende Überwachung von Beschäftigten. Deshalb forderte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits 2014 die Schaffung eines Beschäftigtendatenschutzgesetzes.[2]
Die sich dynamisch entwickelnde Digitalisierung führt zu tiefgreifenden Veränderungen in der Arbeitswelt. Auch vor diesem Hintergrund hat das Bundesministerium für Arbeit und Soziales (BMAS) den interdisziplinären Beirat Beschäftigtendatenschutz eingesetzt, der seinen Abschlussbericht im Januar 2022 fertiggestellt hat. Auch er kommt darin zu dem Schluss, dass – neben weiteren Maßnahmen – ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.[3]
Das europäische Recht ermöglicht es den Mitgliedstaaten spezifischere Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen. Eine erste Regelung hat der deutsche Gesetzgeber mit Erlass des § 26 Bundesdatenschutzgesetz (BDSG) getroffen und sich zugleich weitergehende Regelungen ausdrücklich vorbehalten (BT-Drs. 18/11325, S. 97). Die DSK begrüßt, dass sich im Koalitionsvertrag auf Bundesebene explizit zur Schaffung von Regelungen zum Beschäftigtendatenschutz bekannt wird (Koalitionsvertrag „Mehr Fortschritt wagen“, S. 17).

[2] Entschließung vom 27. März 2014, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20140327_en_Beschaeftigtendatenschutzgesetz.pdf.

[3] Beiratsbericht, S. 6, 9, abrufbar unter: https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf;jsessionid=0A2E14EA95F12CD2F926680929CDC8C5.delivery2-master?__blob=publicationFile&v=3.

Die DSK ist der Auffassung, dass weitergehende Regelungen notwendig und überfällig sind: § 26 BDSG ist nicht hinreichend praktikabel, normenklar und sachgerecht[4]. Die Norm ist als Generalklausel formuliert und eröffnet weite Interpretationsspielräume. Dadurch führt sie zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber, Personalvertretungen oder Gerichte.
Gerade im Zeitalter der Digitalisierung muss ein Beschäftigtendatenschutzgesetz hinreichend flexibel sein, ein hohes Datenschutzniveau gewährleisten sowie Rechtsklarheit für alle Akteure der Arbeitswelt ermöglichen. Zudem hat es insbesondere vor dem Hintergrund der Risiken technischer Entwicklungen einen angemessenen Ausgleich zwischen den grundrechtlich geschützten Interessen der Arbeitgeberinnen und Arbeitgeber sowie dem Recht auf informationelle Selbstbestimmung der Beschäftigten zu schaffen.
Daher fordert die DSK den Gesetzgeber auf, im Rahmen eines eigenständigen Beschäftigtendatenschutzgesetzes mindestens in den folgenden Bereichen gesetzliche Regelungen zu schaffen:

- Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI)

Die Grenzen und Rahmenbedingungen des Einsatzes algorithmischer Systeme im Beschäftigungs- und Bewerbungskontext sollten gesetzlich geregelt werden. Dabei spielt die Schwere, Tiefe und Breite der Grundrechtseingriffe, die der Einsatz algorithmischer Systeme im Beschäftigungskontext typischerweise verursacht, eine wesentliche Rolle. Zudem sind die Hambacher Erklärung der DSK[5] und die von der Datenethikkommission entwickelte „Kritikalitätspyramide“[6] zu berücksichtigen. Je höher die „Kritikalität“, also das Schädigungspotential eines algorithmischen Systems ist, desto strenger sind demnach

[4] S. Stellungnahme der DSK zur Evaluierung des BDSG vom 2.3.2021, S. 8 f., abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf.
[5] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf.
[6] Gutachten der Datenethikkommission, S. 177 ff., abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

die Anforderungen an dessen Einsatz. Im Beschäftigungs- und Bewerbungsverhältnis fallen zahlreiche aussagekräftige Daten an. Die Beschäftigten sowie Bewerberinnen und Bewerber sind wegen ihres Abhängigkeitsverhältnisses besonders schutzbedürftig. Zugleich sollen alle Beteiligten von den Chancen des KI-Einsatzes profitieren können. Korrektur- und Kontrollinstrumente wie Zulassungsverfahren, Vorabprüfungen, Antidiskriminierungs- oder Transparenzvorgaben sowie verbesserte Möglichkeiten der Rechtsdurchsetzung bedürfen daher gesetzlicher Normierung. Besonders eingriffsintensive Datenverarbeitungen sollten verboten werden: So fordert die DSK, auch im Beschäftigungskontext die Profilbildung als solche dem Verbot mit Erlaubnisvorbehalt des Artikels 22 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) zu unterstellen. Es hat sich gezeigt, dass Artikel 22 DS-GVO, dessen Wortlaut nur automatisierte Entscheidungen verbietet, im Beschäftigungskontext nicht ausreichend Schutz gewährleistet. Zum Schutz der betroffenen Bewerberinnen und Bewerber sowie Beschäftigten ist darüber hinaus regelmäßig der Einsatz von KI im Beschäftigungskontext auf der Grundlage einer Einwilligung zu untersagen.

- Grenzen der Verhaltens- und Leistungskontrolle

Die Grenzen der Verhaltens- und Leistungskontrolle bedürfen gesetzlicher Eckpunkte.

Heimliche Kontrollen im Beschäftigungsverhältnis oder Dauerüberwachungen des Verhaltens der Beschäftigten sollten grundsätzlich, im Betrieb ebenso wie im „Home Office“, verboten sein. Die Einzelfallkasuistik der arbeitsgerichtlichen Rechtsprechung und § 26 Absatz 1 Satz 2 BDSG sind im Rahmen einer normenklaren Ausnahmeregelung zu berücksichtigen. Dabei bedarf die Frage, ob § 26 Absatz 1 Satz 2 BDSG auch bei groben Pflichtverletzungen entsprechend Anwendung finden darf, einer gesetzlichen Klarstellung. Gesetzliche Eckpunkte, die z. B. auch Transparenz- und Zertifizierungsanforderungen für technische Anwendungen vorgeben können, sind insbesondere zu folgenden Aspekten nötig:

Grenzen des Zugriffs auf und der Auswertung von E-Mails, Internetdienstdaten und weiteren IT-Daten der Beschäftigten durch Arbeitgeberinnen und Arbeitgeber, Regelungen zum Einsatz von Videoüberwachungssystemen sowie Grenzen des Einsatzes von Geoinformationssystemen (GPS-Tracking) und biometrischen Verfahren im Beschäftigungsverhältnis. Hintergrund ist, dass der Einsatz und die Auswertung von Informations- und Kommunikationstechnologie gerade

bei computergebundenen Arbeitsplätzen weitreichende Möglichkeiten der Leistungsüberwachung der Beschäftigten eröffnet, die durch gesetzliche Regelungen beschränkt werden müssen. Auch die Auswertung und Analyse von mit GPS ausgestatteten Fahrzeugen hat hohes Überwachungspotential und bedarf einer Regulierung. Besonders schützenswerte persönliche Merkmale wie biometrische Daten von Beschäftigten dürfen nur in Ausnahmefällen, die der Gesetzgeber definieren sollte, für Zwecke des Beschäftigungsverhältnisses genutzt werden.

- Ergänzungen zu den Rahmenbedingungen der Einwilligung

Die DSK befürwortet eine Ergänzung der Regelungen des § 26 Absatz 2 BDSG unter Berücksichtigung der Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung, wonach die Einwilligung im Beschäftigungsverhältnis wegen des bestehenden Machtungleichgewichts grundsätzlich kritisch zu sehen ist[7]. Zudem sollte die entsprechende Regelung die Formulierung von Regelbeispielen bzw. Bedingungen enthalten, in welchen Fällen Einwilligungen im Beschäftigungs- und Bewerbungsverhältnis unzulässig sein sollen.

- Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen

Die DSK fordert den Gesetzgeber auf klarzustellen, ob und inwieweit mit Kollektivvereinbarungen einschließlich Betriebsvereinbarungen zusätzliche Rechtsgrundlagen für Datenverarbeitungen im Beschäftigungsverhältnis geschaffen werden können. Der Wortlaut von Artikel 88 Absatz 1 DS-GVO und § 26 Absatz 1 Satz 1 BDSG ist in dieser Hinsicht unklar.

- Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Artikel 6 und 9 DS-GVO

Die DSK empfiehlt, eindeutige konkretisierende Regelungen für die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, im Beschäftigungsverhältnis zu schaffen. Denn die Anwendungsbereiche der Regelungen des § 22 BDSG und des § 26 BDSG überschneiden sich: Unklar ist, welcher der beiden Paragraphen den Vorrang genießt. Nach § 22 Absatz 1 Nummer 1 Buchstabe b BDSG ist beispielsweise die Verarbeitung besonderer

[7] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4.5.2020, Rdnr. 21 ff., abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

Kategorien personenbezogener Daten „für die Beurteilung der Arbeitsfähigkeit des Beschäftigten“ zulässig. Dieser steht hinsichtlich des Anwendungsbereiches nicht im Einklang mit § 26 Absatz 3 BDSG, der die Verarbeitung besonderer Kategorien von personenbezogenen Daten im Beschäftigungsverhältnis an weitere Bedingungen knüpft.
Unklar ist darüber hinaus auch das Verhältnis zu Artikel 6 Absatz 1 und Artikel 9 Absatz 2 DS-GVO hinsichtlich der Frage, inwiefern auf die Ermächtigungsgrundlagen aus der DS-GVO zurückgegriffen werden darf, wenn die Verarbeitung gemäß § 26 BDSG ausgeschlossen ist. Es ist hinsichtlich der neu zu schaffenden bereichsspezifischen Rechtsgrundlagen daher notwendig, ihr Verhältnis zu den Rechtsgrundlagen der DS-GVO klarzustellen.

- Beweisverwertungsverbote

Die DSK befürwortet die gesetzliche Normierung eines Beweisverwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten. Diese Regelung sollte klare Kriterien für das Vorliegen eines Beweisverwertungsverbotes enthalten.

- Datenverarbeitung bei Bewerbungs- und Auswahlverfahren

Die DSK ist der Ansicht, dass gesetzliche Regelungen zur Datenverarbeitung in der Bewerbungsphase erforderlich sind. Geregelt werden sollten die Möglichkeiten und Grenzen der Verarbeitung von direkt bei Bewerberinnen und Bewerbern sowie bei Dritten oder aus öffentlich zugänglichen Quellen in Bezug auf die Bewerberinnen und Bewerber erhobenen Daten. Darunter fallen insbesondere die folgenden Themenkomplexe: Fragerecht der Arbeitgeberinnen und Arbeitgeber, Anforderung polizeilicher Führungszeugnisse, ärztliche Untersuchungen und Eignungstests, Datenerhebung aus Drittquellen (z. B. bei vorherigen Arbeitsstellen), Umgang mit sozialen Netzwerken oder das sog. Active Sourcing. Wesentlich sind in dieser Phase auch Regelungen zur Transparenz und klare Löschfristen.

4.4 Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 24. November 2022

Vorbemerkung
Die wissenschaftliche Forschung mit Gesundheitsdaten, also mit Informationen über den Gesundheitszustand von Personen, kann dazu dienen, Erkenntnisse über die Ursachen von Krankheiten zu gewinnen, effiziente Therapien zu entwickeln und Behandlungsmöglichkeiten zu verbessern.
Damit steht sie im essentiellen Interesse der Allgemeinheit und sollte gerade bei der Verfolgung dieser Ziele bestmöglich gefördert werden. Allerdings ist dabei zu beachten, dass die hierfür relevanten Datenkategorien von der europäischen Datenschutz-Grundverordnung (DSGVO) in besonderer Weise geschützt werden und einem besonders hohen Schutzbedarf unterliegen. Eine unsachgemäße Verwendung sensibler Gesundheitsdaten kann zu gravierenden Folgen führen, wie z.B. soziale Stigmatisierung oder sogar Diskriminierung für die betroffenen Personen etwa auf dem Arbeits- und Versicherungsmarkt.
Datenverarbeitung für Zwecke der wissenschaftlichen Forschung genießt schon heute in der Datenschutz-Grundverordnung und den nationalen Datenschutzgesetzen eine weitgehende Privilegierung. Es ist daher eine wichtige Herausforderung, Wege und Lösungen zu finden, um die Verarbeitung von Gesundheitsdaten zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken zu ermöglichen und ihre Vorzüge nutzbar zu machen. Gleichzeitig ist den damit verbundenen Risiken konsequent zu begegnen, um den Betroffenen einen adäquaten Grundrechtsschutz zu gewähren.
Mit begründetem Vertrauen der betroffenen Personen in die Einhaltung ethischer, rechtlicher und technischer Standards wächst ihre Motivation, die Forschung zu unterstützen. Deshalb ist es für Bürgerinnen und Bürger unerlässlich, darauf vertrauen zu können, dass ihre personenbezogenen Daten im Einklang mit den sie schützenden datenschutzrechtlichen Vorgaben und unter Wahrung ihrer informationel-

len Selbstbestimmung verarbeitet werden. Auch deshalb ist Datenschutz eine Voraussetzung für eine menschenzentrierte wissenschaftliche Forschung mit Gesundheitsdaten.
Grundlage für eine solche datenschutzkonforme effektive Gesundheitsdatenforschung ist neben einer weitreichenden Transparenz vor allem eine hohe Rechtsklarheit für alle Beteiligten sowie die Sicherstellung eines nachhaltigen Schutzes personenbezogener Daten, wie bereits in ihrer Entschließung vom 23. März 2022 „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“ von der DSK gefordert.
In Konkretisierung dieser Forderungen hat sich die DSK auf die folgenden Empfehlungen im Zusammenhang mit der Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung verständigt:

1. **Die Menschen stehen im Mittelpunkt der Forschung. Sie dürfen nicht zum bloßen Objekt der Datenverarbeitung gemacht werden. Entsprechende Verarbeitungsprozesse müssen daher rechtmäßig sowie für betroffene Personen stets transparent und nachvollziehbar sein. Auch wenn eine Verarbeitung ihrer Daten im öffentlichen Interesse gesetzlich erlaubt und nicht auf ihre Einwilligung gestützt wird, sind die betroffenen Personen in geeigneter Form einzubinden. Digitale Managementsysteme sollen Informations-, Kontroll- und Mitwirkungsmöglichkeiten sicherstellen. Gesetzliche Regelungen müssen wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen.**
2. **Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten genutzt werden.**
3. **Zu den grundlegenden Garantien und Maßnahmen gehören die Verschlüsselung, die Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung. Zusätzlich sind besondere Anforderungen bei Verarbeitungen in Drittländern zu beachten. Anonyme Datensätze, die die Re-Identifikation auch für Personen mit Zusatzwissen irreversibel ausschließen, können Forschende umfassend nutzen.**

4. **Auswertungen anhand von Falldaten greifen insbesondere dann besonders tief in die Rechte und Freiheiten der betroffenen Personen ein, wenn Datensätze aus verschiedenen Quellen verknüpft werden. Daher müssen die Art und der Umfang der Bereitstellung, der Zweck der Auswertung und die Forschenden persönlich besondere Schutzanforderungen erfüllen. Geeignete Verfahren müssen gewährleisten, dass rechtliche und technische Voraussetzungen für den Datenzugang erfüllt sind. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos festzulegen, damit betroffene Personen ihre Datenschutzrechte ausüben können.**
5. **Mit einem zentralen Registerverzeichnis sollten die Nutzung der in den verschiedenen Registern gespeicherten Daten für alle Beteiligten transparent gestaltet und mehrfache Datensammlungen vermieden werden. Dabei sind Qualitätsanforderungen verbindlich vorzugeben, zu prüfen und auszuweisen. Zudem sollte eine zentrale koordinierende Stelle mit Lotsenfunktion geschaffen werden, die Datennutzungsanträge veröffentlicht und die Nutzenden zur Publizierung der Forschungsergebnisse in anonymer Form verpflichtet. Dies schafft sowohl Wissen im Allgemeininteresse als auch Schutz für die betroffenen Personen.**
6. **Durch eine gesetzliche Regelung des Forschungsgeheimnisses ist der Umgang mit personenbezogenen medizinischen Forschungsdaten für wissenschaftlich Forschende auch in strafrechtlicher und prozessualer Sicht klarzustellen und damit ein wichtiger Beitrag zum Schutz dieser Daten zu leisten.**
7. **Die Datenschutzbehörden müssen die Einhaltung datenschutzrechtlicher Anforderungen umfassend und effektiv überwachen und durchsetzen können. Hierfür ist auch erforderlich, gegenüber öffentlichen Stellen den sofortigen Vollzug von Maßnahmen anordnen zu können. Zur Erleichterung der Kontrolle sollten standardisierte Anforderungen u.a. an die Dokumentation der Datenverarbeitungsprozesse festgelegt werden.**

Grundlage für die Datenverarbeitung

Generell gilt: Die Einzelperson darf nicht zum bloßen Objekt der Datenverarbeitung gemacht werden.

Ungeachtet der gesondert zu führenden Diskussionen zum europäischen Gesundheitsdatenraum und zur Nutzung von Gesundheitsdaten

zu Forschungszwecken auf europäischer Ebene, besteht nach Auffassung der DSK auch auf nationaler Ebene Bedarf, die Regelungen für die Nutzung von Forschungsdaten näher zu spezifizieren und kohärent auszugestalten. Ziel dabei sollte eine länderübergreifende, einheitliche Regelung zur Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken sein, die Forschungsverbünden mit Partnern in unterschiedlichen Bundesländern das Einhalten der datenschutzrechtlichen Anforderungen erleichtert.
Soweit Ärztinnen und Ärzte und andere Berufsgeheimnisträger ermächtigt werden sollen, personenbezogene Daten zu Forschungszwecken zu übermitteln, muss die Regelung mit dem Berufsrecht in Einklang stehen.
Die datenschutzrechtliche Einwilligung als Grundlage für die Datennutzung kann dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen. Sie muss freiwillig erfolgen, setzt eine umfassende Information voraus und ist jederzeit widerruflich.
Es ist Aufgabe des Gesetzgebers, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen, aber auch ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren. Der Gesetzgeber darf diese komplexen Fragestellungen nicht vollständig auf die betroffenen Personen und die Forschenden verlagern.
Sofern eine gesetzliche Regelung Rechtsgrundlage einer Datenverarbeitung zu Forschungszwecken sein soll, muss sie in jedem Fall normenklar wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen. Eine solche Regelung kann bei der Nutzung von Daten aus anderen Quellen, beispielsweise Behandlungsdaten aus Krankenhäusern, aus medizinischen Registern oder auch aus anderen Forschungsprojekten (sog. Sekundärnutzung) datenschutzkonforme Forschung ermöglichen oder erleichtern, wenn das Einholen einer ausdrücklichen Einwilligung nicht durchführbar wäre oder das Forschungsvorhaben ernsthaft beeinträchtigen würde.
Zweck der wissenschaftlichen Forschung
Eine gesetzliche Grundlage für die Nutzung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken muss einen Ausgleich insbesondere zwischen den verfassungsrechtlich geschützten Interessen schaffen: dem Recht der betroffenen Personen auf Kontrolle über ihre Daten (sog. „informationelles Selbstbestimmungsrecht“) einerseits

und der Forschungsfreiheit der Wissenschaftler und wissenschaftlichen Einrichtungen andererseits.
Eine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken sollte im Rahmen der Interessenabwägung u.a. Gemeinwohlinteressen – insbesondere das öffentliche Interesse an den Erkenntnissen und den Nutzen für die Allgemeinheit – berücksichtigen. Es bedarf der näheren Bestimmung durch den Gesetzgeber, was inhaltlich der Forschung im Gemeinwohlinteresse entspricht und welche weiteren Anforderungen an das Verfahren und die Durchführung der Forschung gestellt werden.
Geeignete Garantien für die Rechte und Freiheiten betroffener Personen
Eine gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten muss angemessene Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen enthalten.
Die Privilegierung der Forschung als Zweck der Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung wird flankiert von zusätzlichen Anforderungen, vor allem zur Datenminimierung und zur frühestmöglichen Anonymisierung. Da die Anonymisierung den besten Schutz für die Rechte und Freiheiten der betroffenen Personen bietet, ist die Umsetzung dieser Schutzmaßnahme immer vorrangig zu prüfen.
Soweit der Forschungszweck mit anonymisierten Daten erreicht werden kann, dürfen nur anonymisierte Daten verarbeitet werden. Dabei bestehen hohe Anforderungen an die Anonymisierung personenbezogener Daten. Soweit zur Erreichung des Forschungszwecks eine vollständige Anonymisierung nicht möglich ist, sind effektive Maßnahmen der Pseudonymisierung vorzusehen. Darüber hinaus sind technische und organisatorische Schutzmaßnahmen entsprechend dem für die bei Gesundheitsdaten gesteigerten Anforderungen gemäß dem Stand der Technik zu treffen, darunter solche zur Pseudonymisierung und Verschlüsselung der Daten.
Falls Datenverarbeitungen auch in Ländern außerhalb des Europäischen Wirtschaftsraums stattfinden sollen, entstehen dadurch Risiken, denen mit besonderen Garantien zu begegnen ist. Dies ist nach der DSGVO gewährleistet mit Beschlüssen nach Art. 45 DSGVO und bei Garantien nach Art. 46 DSGVO einschließlich gebotener ergänzender Maßnahmen. Auch in allen anderen Fällen sollten Pseudonymisierungen oder Verschlüsselungen ausschließen, dass die Daten im Drittland einer spezifischen Person zugeordnet werden können.

Pseudonymisierung durch Vertrauensstellen
Die Aufgabe der Pseudonymisierung der Gesundheitsdaten sollte gesetzlich an unabhängige und eigenverantwortliche Vertrauensstellen übertragen werden. Dafür ist entscheidend, diese Stellenvöllig unabhängig auszugestalten und insbesondere Weisungen von wissenschaftlich Forschenden bzgl. der von den Vertrauensstellen verarbeiteten Daten auszuschließen. Die konkreten Aufgaben, Rechte und Pflichten der Vertrauensstellen sind zu definieren. Je nach Ausgestaltung ist zudem die eigene Verantwortlichkeit dieser Stellen für die Datenverarbeitung im Interesse der Wahrung der Betroffenenrechte festzulegen.
Kontrolle durch die betroffenen Personen: Mitwirkung und Widerspruch
Will der Gesetzgeber die Verarbeitung zu Forschungszwecken nicht auf eine Einwilligung, sondern auf eine gesetzliche Grundlage stellen, sollte er die Einbindung der betroffenen Personen vorsehen. Dabei ist zumindest sicherzustellen, dass die betroffene Person in der Regel einer Verarbeitung der personenbezogenen Daten zu Forschungszwecken voraussetzungslos widersprechen kann. Ausnahmen können nur für gesetzlich konkret bestimmte Einzelfälle vorgesehen werden, wenn dieses Recht den Forschungszweck unmöglich macht oder ernsthaft beeinträchtigt. Das Verfahren ist so auszugestalten, dass der Widerspruch möglichst unkompliziert ausgeübt werden kann.
Die betroffenen Personen müssen über die Verarbeitungsschritte informiert werden sowie Gelegenheit erhalten, sich leicht zu informieren. Digitale Methoden oder Managementsysteme, wie Datencockpit, Dashboard oder Portal, sollen dabei Information, Kontrolle und Mitwirkung vereinfachen, indem sie Nachrichten übermitteln und digitale Einwilligungserklärungen zulassen. Durch entsprechende Vorgaben sollten Lösungen erreicht werden, die Bürgerinnen und Bürgern einheitliche und leicht zugängliche Wege bieten, ihre Kontrollrechte auszuüben.
Sichere Datenbereitstellung
Zunächst ist ein Verfahren festzulegen, in dem zuverlässig überprüft werden kann, ob ein Zugriff auf die Daten datenschutzrechtlich zulässig ist (Use-and-Access-Verfahren). Bei der Bereitstellung von personenbezogenen Daten für Forschende müssen besondere technische und organisatorische Anforderungen vorgeschrieben werden. So sollte ein Zugang zu den Daten vorrangig in einer sicheren Umgebung der Zugangsstelle vorgesehen werden. Ein Zugriff oder Abruf sollte

nur dann möglich sein, wenn Forschende zuvor nachweisen, dass sie angemessene technische und organisatorische Maßnahmen implementiert haben und den Stand der Technik einhalten.
Um den Verantwortlichen Hilfestellung zur Beachtung einheitlicher Mindeststandards zu geben, sollten generelle Risiken der Verarbeitung im Wege einer gesetzlichen Datenschutz-Folgenabschätzung ermittelt und berücksichtigt sowie grundlegende Maßnahmen zur Risikominimierung unmittelbar gesetzlich geregelt werden. Unabhängig davon ist von den Verantwortlichen eine Datenschutz-Folgenabschätzung für jeweils bevorstehende Forschungsvorhaben durchzuführen.
Verknüpfung von Datensätzen
Sofern eine gesetzliche Grundlage geschaffen werden sollte, um Datensätze aus verschiedenen Quellen, beispielsweise aus medizinischen Registern, zu verknüpfen, sind besondere Sicherheits- und Schutzmaßnahmen vorzusehen. Die Verknüpfung erhöht das Risiko für die Rechte und Freiheiten natürlicher Personen, wenn sie anhand der zusammengeführten Informationen leichter zu identifizieren sind. Sie verstärkt darüber hinaus das Risiko, dass Zweckbindungen nicht eingehalten werden, dass zusätzliche, nicht zur Erreichung des Forschungszwecks erforderliche Informationen in einer für die betroffenen Personen wenig überschaubaren Weise generiert oder auch unrichtige Informationen erzeugt werden. Es sind besondere Record-Linkage-Verfahren vorzusehen, die nur eine anlassbezogene und temporäre Zusammenführung zulassen sollten. Die betroffenen Personen sollten über ein Einwilligungsmanagementsystem die Gelegenheit haben, in Kenntnis der Risiken der Zusammenführung aktiv zuzustimmen. Alternativ müssen technische Methoden oder Maßnahmen sicherstellen, dass die Reidentifizierung der betroffenen Person trotz der Verkettung ausgeschlossen ist.
Bei der Verarbeitung von Daten zu Forschungszwecken muss stets unter Beachtung der vorliegenden Risiken geprüft werden, ob und inwieweit Daten zentral oder dezentral gespeichert oder verarbeitet werden. Soweit dies vom Forschungszweck her möglich ist, sollten die Daten am Ort der Speicherung ausgewertet werden, so dass den Ort der sicheren Speicherung nur anonyme Ergebnisse der Datenauswertung verlassen. Dabei ist eine Mehrfachspeicherung zu vermeiden.
Partizipation und Teilnahme
Im Zusammenhang mit der Gesundheitsforschung gibt es bereits vielfältige Ansätze zur Partizipation der betroffenen Personen. Einige

Forschungsvorhaben und Register ermöglichen den betroffenen Personen, sich über Vorhaben und daraus resultierende Erkenntnisse z.B. zu Behandlungsalternativen oder Therapien zu informieren, darüber zu diskutieren und sich bestimmte Forschungsthemen zu wünschen. Diese Partizipation sollte gesetzlich verankert werden.
Denkbar sind Webportale mit weiterführenden Informationen über konkrete Forschungsprojekte sowie einzelne darauf bezogene Krankheitsbilder und in diesem Zusammenhang stehende Therapieziele, Diskussionsforen, Newsletter oder Veröffentlichungen von Datenauswertungen.

Klare Verantwortlichkeiten

Die DSK empfiehlt, gesetzlich zu bestimmen, wer datenschutzrechtlich für einzelne Verarbeitungsschritte verantwortlich ist. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos zu regeln, insbesondere bei der Übermittlung zwischen Forschungseinrichtungen, um sicherzustellen, dass die betroffenen Personen ihre Datenschutzrechte ausüben können. Es sind rechtsklare Regelungen zur Aufbewahrungsdauer und Löschung von Forschungsdaten festzulegen, die sowohl das Recht auf informationelle Selbstbestimmung der betroffenen Personen als auch das Interesse der wissenschaftlichen Forschung an einer späteren Überprüfbarkeit der Forschungsergebnisse berücksichtigen. Die aus Sicht des Datenschutzes besonders relevanten Instrumente der Verschlüsselung, Pseudonymisierung und Anonymisierung sollten vom Gesetzgeber präzisiert werden.

Daten aus medizinischen Registern

Eine gesetzliche Regelung zur Nutzung von personenbezogenen Daten für Forschungszwecke sollte zudem spezifische Vorgaben für medizinische Register schaffen. Sie sollte einheitliche Anforderungen für die Datenverarbeitung in den Registern enthalten.
Hierzu sollte zunächst ein laufendes, zentrales Verzeichnis der bestehenden Register im Gesundheitsbereich errichtet werden, um eine strukturierte Übersicht über vorhandene Daten zu bieten. Dies schafft für die betroffenen Personen ebenso wie für die Forschenden Transparenz. Zugleich vermeidet dies mehrfache Datensammlungen mit gleichen Inhalten und fördert so den Grundsatz der Datenminimierung.
Weiter sind Standards für die Qualität medizinischer Register und der dortigen Verarbeitung festzulegen, die auch Vorgaben zum Datenschutz und zur Datensicherheit enthalten müssen. So sollten die von

den Registern einzuhaltenden technisch-organisatorischen Maßnahmen harmonisiert werden. Zugleich sollte ein Verfahren vorgesehen werden, mit dem die Einhaltung dieser Standards – in regelmäßigen Abständen wiederholt – geprüft und nachgewiesen wird.
Eine Datenverarbeitung in den Registern ist stets nur zulässig, wenn die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet ist. Eine Befugnis zur Übermittlung von personenbezogenen Daten, insbesondere Patientendaten, in ein Register setzt dabei mindestens die normenklare Definition des Datenkranzes und die Erforderlichkeit der Erfassung aus medizinisch-fachlicher Sicht voraus. Eine ausdrückliche Meldepflicht ist nur in besonderen Ausnahmefällen denkbar und muss aus verfassungsrechtlichen Gründen gesetzlich festgelegt sein.
Sollte eine zentrale, koordinierende Stelle vorgesehen werden, könnte diese hinsichtlich der Betroffenenrechte eine Beratungs- und Lotsenfunktion wahrnehmen. Um die zuverlässige Durchführung dieser Aufgaben zu gewährleisten, ist eine öffentliche Stelle hiermit zu betrauen und die datenschutzrechtliche Verantwortlichkeit der Stelle ebenso wie die datenschutzrechtliche Aufsicht eindeutig festzulegen.
Normenklare Regelung eines Forschungsgeheimnisses
Bereits mit ihrer Entschließung im Jahr 2004 hat die 67. DSK die Einführung eines Forschungsgeheimnisses gefordert und diese Forderung im März 2022 bekräftigt. Hierdurch sollte die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe gestellt, deren Beschlagnahme verboten und ein Zeugnisverweigerungsrecht für wissenschaftlich Forschende und ihre Berufshelfer geschaffen werden. Die DSK erinnert eindringlich an diese Forderung und ist bereit, entsprechende Vorhaben beratend zu begleiten.
Überwachung und Aufsicht
Die unabhängigen Datenschutz-Aufsichtsbehörden müssen die Einhaltung der datenschutzrechtlichen Regelungen zur Verarbeitung personenbezogener Gesundheitsdaten im Forschungskontext lückenlos überwachen und durchsetzen können. Sie müssen auch gegenüber öffentlichen Stellen mit Befugnissen ausgestattet werden, erforderliche Anordnungen durchsetzen zu können. Dazu gehört auch die – europarechtlich ohnehin gebotene und in Deutschland bisher ausgeschlossene – Möglichkeit, sofortigen Vollzug von Maßnahmen anordnen zu können.
Um eine effektive und konstruktive Aufsicht zu gewährleisten, sind konkrete Anforderungen an die prüffähige Dokumentation der Verar-

beitungsschritte und die zu implementierenden technischen und organisatorischen Maßnahmen vorzusehen. Ebenso sind die forschenden Einrichtungen mit ausreichendem datenschutzrechtlichen Sachverstand auszustatten.

4.5 Zur Task Force Facebook-Fanpages

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 23. März 2022

Die DSK nimmt das von der Taskforce Facebook-Fanpages erstellte Kurzgutachten zur Frage der datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 18.03.2022 zur Kenntnis und stimmt der Bewertung zu.
Es bildet für die Mitglieder der DSK eine wichtige Grundlage ihrer aufsichtsbehördlichen Tätigkeit gegenüber öffentlichen und nichtöffentlichen Stellen.
Aufgrund ihrer Vorbildfunktion stehen öffentliche Stellen zuvörderst im Fokus. Deshalb werden die Mitglieder der DSK im Rahmen ihrer Zuständigkeit

- die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zeitnah informieren,
- überprüfen, ob Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben,
- darauf hinwirken, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.
  Dieser Nachweis betrifft vor allem
- den Abschluss einer Vereinbarung nach Art. 26 DSGVO über die gemeinsame Verantwortlichkeit mit Facebook,
- ausreichende Informationen über die gemeinsamen Datenverarbeitungen gegenüber den die Fanpages Nutzenden gemäß Art. 13 DSGVO,
- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie

- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten.

Hinweis: Der Beschluss wurde mehrheitlich mit einer Gegenstimme gefasst. Die Gegenstimme richtet sich gegen die Ausführungen des dritten Absatzes.

4.6 Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 24. März 2022

Auch im Online-Handel gilt der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Danach sind nur die Daten zu erheben, die für die Abwicklung eines einzelnen Geschäfts erforderlich sind. Die zulässige Verarbeitung der personenbezogenen Daten hängt im Einzelfall insbesondere davon ab, ob Kund*innen einmalig einen Vertrag abschließen wollen oder eine dauerhafte Geschäftsbeziehung anstreben. Dazu müssen Kund*innen jeweils frei entscheiden können, ob sie ihre Daten für jede Bestellung eingeben und insofern als sogenannter temporärer Gast geführt werden möchten oder ob sie bereit sind, eine dauerhafte Geschäftsbeziehung einzugehen, die mit einem fortlaufenden Kund*innenkonto verbunden ist.
Daraus ergibt sich Folgendes:
1. Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, müssen ihren Kund*innen unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kund*innenkonto) zur Verfügung stellen, grundsätzlich einen Gastzugang (Online-Geschäft ohne Anlegen eines fortlaufenden Kund*innenkontos) für die Bestellung bereitstellen.
Im Online-Handel ist das **fortlaufende Kund*innenkonto** regelmäßige Praxis. Es wird unter Vergabe von Zugangsdaten (z. B. Benutzername/Passwort) eingerichtet, um sich gegenüber dem Verantwortlichen eindeutig zu identifizieren. Kund*innen können damit auf ein bei dem Verantwortlichen geführtes Kund*innenkonto selbst und aktiv zugreifen, um ggf. ihre Daten zu ändern oder Bestellungen zu prüfen. Fortlaufende Kund*innenkonten werden über den erstmaligen

Geschäftsabschluss hinaus im Aktivdatenbestand gepflegt. Sie dienen den Kund*innen zur vereinfachten wiederkehrenden Bestellmöglichkeit ohne die nochmalige Eingabe aller personenbezogenen Daten. Darüber hinaus kann ein fortlaufendes Kund*innenkonto eine Bestell- oder Geschäftshistorie vorsehen, die dem Verantwortlichen eine Auswertung zur Profilbildung und für Werbezwecke ermöglicht.
Nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist nur die Verarbeitung der personenbezogenen Daten zulässig, die für die Erfüllung des einzelnen Vertrages erforderlich sind. Bei einer erstmaligen Bestellung kann der Verantwortliche nicht per se unterstellen, dass er Daten von Kund*innen für mögliche, aber ungewisse zukünftige Geschäfte auf Vorrat vorhalten darf. Für die Einrichtung eines fortlaufenden Kund*innenkontos ist eine entsprechende bewusste Willenserklärung der Kund*innen erforderlich. Für Kund*innen, die keine dauerhafte Geschäftsbeziehung eingehen wollen oder eine Verarbeitung von nicht zur Geschäftsabwicklung benötigten Daten ablehnen, ist daher regelmäßig ein **Gastzugang** zu ermöglichen. Ein solcher Zugang verzichtet auf Registrierungs- bzw. Zugangsdaten (z. B. Benutzername/Passwort) für eine erneute Nutzung. Über diesen Zugang dürfen nur die zur Durchführung des Vertrages und zur Erfüllung gesetzlicher Pflichten erforderlichen personenbezogenen Daten und Informationen der Kund*innen erfasst werden. Nach Vertragserfüllung nicht mehr benötigte Daten müssen gemäß Art. 17 Abs. 1 Buchstabe a) DS-GVO unverzüglich gelöscht werden. Werden die Daten im Übrigen nur noch im Rahmen spezialgesetzlich geregelter Aufbewahrungsplichten verarbeitet, z. B. aus dem Handels- oder Steuerrecht, sind technisch-organisatorische Maßnahmen zu ergreifen, um diese Daten von den Daten im operativen Zugriff zu trennen (Datensperrung). Ein Zugriff der Kund*innen auf die Daten oder das Hinzuspeichern von weiteren Daten durch die Verantwortlichen sind bei einem Gastzugang nicht vorgesehen.
Soweit im Einzelfall besondere Umstände vorliegen, bei denen ein fortlaufendes Kund*innenkonto ausnahmsweise als für die Erfüllung eines Vertrages erforderlich angesehen werden kann (Art. 6 Abs. 1 Buchstabe b) DS-GVO, z. B. für Fachhändler bei bestimmten Berufsgruppen) und mithin hierfür ausnahmsweise keine Einwilligung erforderlich ist, ist dem Grundsatz der Datenminimierung Rechnung zu tragen, indem z. B. das Kund*innenkonto bei Inaktivität automatisiert nach einer kurzen Frist gelöscht wird.

2. Ohne einen Gastzugang bzw. ohne eine gleichwertige Bestellmöglichkeit kann die Freiwilligkeit einer Einwilligung nicht gewährleistet werden.

Damit eine für die Einrichtung eines fortlaufenden Kund*innenkontos erforderliche Einwilligung nicht gegen die in Art. 7 Abs. 4 DS-GVO erwähnte Konditionalität verstößt, müssen die Kund*innen im Online-Shop auch die gleichen Angebote auf anderem gleichwertigen Wege als über das fortlaufende Kund*innenkonto bestellen können (vgl. Rn. 37 f. der Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des Europäischen Datenschutzausschusses vom 04.05.2020). Gleichwertig ist eine Bestellmöglichkeit, wenn keinerlei Nachteile entstehen, also Bestellaufwand und Zugang zu diesen Möglichkeiten, wie bei einem Gastzugang, denen eines laufenden Kund*innenkontos entsprechen und technisch organisatorische Maßnahmen getroffen werden, die ein angemessenes Datenschutzniveau gewährleisten.

3. Die mit einem fortlaufenden Online-Konto verbundenen Möglichkeiten der Auswertung der Vertragshistorie für Werbezwecke so wie die Speicherung von Informationen über Zahlungsmittel bedürfen einer informierten Einwilligung.

Sollen in einem fortlaufenden Kund*innenkonto die über die Kontaktdaten hinausgehenden personenbezogenen Daten, ggf. einschließlich der Vertragsdaten der Bestellungen, für Werbezwecke (Profiling der Kundenhistorien, Zusammenführung mit Daten aus anderen Quellen) ausgewertet und verarbeitet werden, sind darauf bezogen Einwilligungen der Kund*innen nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO einzuholen. Da dies eine Verarbeitung ist, die über die bloße Einrichtung und Führung eines fortlaufenden Kund*innenkontos hinausgeht, ist diese nicht bereits durch eine Einwilligung zur Einrichtung und Führung des fortlaufenden Kund*innenkontos abgedeckt. Da Kund*innen, die einen Gastzugang wählen, damit regelmäßig zugleich zu erkennen geben, dass sie eine Werbeansprache ablehnen, ist eine andere Rechtsgrundlage für diese Datennutzung nicht ersichtlich. Gleiches gilt für das Speichern etwaiger Zahlungsmittel wie Kreditkarten. Siehe dazu die Empfehlungen des EDSA 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen.

4. Die von den Verantwortlichen verarbeiteten Daten müssen in einer für die Kund*innen transparenten Weise verarbeitet werden.

Verantwortliche haben sowohl bei Einrichtung eines Gastzugangs als auch bei Einrichtung des fortlaufenden Kund*innenkontos ihre Informationspflichten bei erstmaliger Datenerhebung zu erfüllen. Die Einrichtung des fortlaufenden Kund*innenkontos im Wege einer Einwilligung nach Art. 6 Abs. 1 S. 1 Buchstabe a) DS-GVO setzt zusätzlich voraus, dass diese in informierter Weise erfolgt.
Sowohl für die Einwilligung gemäß Art. 7 DS-GVO, als auch bei einer für die Vertragserfüllung erforderlichen Datenverarbeitung sind die Kund*innen in verständlicher Sprache über die Einzelheiten der Datenverarbeitung zu informieren (Art. 7 Abs. 2 und Art. 12 - 14 DS-GVO).

4.7 Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 13. April 2022

Für gesetzlich bestimmte Einrichtungen und Unternehmen aus dem Gesundheitsbereich gilt seit dem 15. März 2022 eine einrichtungsbezogene Impfpflicht, § 20a Absatz 1 IfSG. Seit diesem Zeitpunkt dürfen in diesen nur Personen tätig sein, die gegen das Coronavirus SARS-CoV-2 geimpft oder von diesem genesen sind oder bei denen eine medizinische Kontraindikation hinsichtlich einer Impfung gegen das Coronavirus SARS-CoV-2 vorliegt.
Für die genannten Personen besteht eine Nachweispflicht über ihre Impfung, Genesung oder das Vorliegen einer medizinischen Kontraindikation, § 20a IfSG.

- **Für wen genau gilt die einrichtungsbezogene Impfpflicht?**
  Die einrichtungsbezogene Impfpflicht gilt für alle Personen, die in den in § 20a IfSG benannten Einrichtungen/Unternehmen tätig sind. Dies sind nicht allein die unmittelbaren Beschäftigten, sondern auch weitere vor Ort tätige Personen, wie Handwerker, Leiharbeitnehmerinnen und Leiharbeitnehmer, Praktikantinnen und Praktikanten usw.
  Der Wortlaut der gesetzlichen Regelung lässt offen, ob diese auch auf Arbeitskräfte Anwendung findet, die sich nur kurze Zeit im

Gebäude aufhalten. Bitte wenden Sie sich in Zweifelsfällen an die für die Anwendung des Infektionsschutzgesetzes für Sie zuständige jeweilige öffentliche Stelle.

- **Was gilt als Nachweis über eine Impfung, Genesung oder medizinische Kontraindikation?**
  Was im Einzelnen als Nachweis für die Impfung und Genesung gilt, ist wiederum in § 22a Absatz 1 und Absatz 2 IfSG geregelt. Der vorgelegte Nachweis muss den genannten Regelungen entsprechen, § 20a Absatz 2 Nummer 1 und 2 IfSG.
  Als Nachweis über eine medizinische Kontraindikation gilt ein ärztliches Zeugnis darüber, dass die betroffene Person auf Grund einer medizinischen Kontraindikation nicht gegen das Coronavirus SARS-CoV-2 geimpft werden kann, § 20a Absatz 2 Nummer 4 IfSG. Nach dem Wortlaut des Gesetzes ist es ausreichend, dass in dem ärztlichen Zeugnis das Vorliegen einer medizinischen Kontraindikation an sich bestätigt wird. Konkrete Gesundheitsdaten, wie Diagnosen, dürfen seitens der Leitung der unter § 20a IfSG fallenden Einrichtung/des Unternehmens nicht gefordert werden.
  Sollte es sich bei den medizinischen Kontraindikationen lediglich um vorübergehende handeln, wird in dem Zeugnis voraussichtlich auch ein Enddatum für das Vorliegen der medizinischen Kontraindikation benannt sein.
  Alternativ können schwangere Personen, die in den in § 20a IfSG benannten Einrichtungen/Unternehmen tätig sind, ein ärztliches Zeugnis darüber vorlegen, dass sie sich im ersten Schwangerschaftsdrittel befinden, § 20a Absatz 2 Nummer 3 IfSG.
- **Gegenüber wem ist der Nachweis über eine Impfung, Genesung oder medizinischen Kontraindikation zu erbringen?**
  Der Nachweis ist gegenüber der Leitung der Einrichtung/des Unternehmens zu erbringen, § 20a Absatz 2 IfSG. Zum Begriff der „Leitung“ siehe auch § 2 Nummer 15a, b IfSG.
  Auch Personen, die nicht unmittelbar in einem Arbeitsverhältnis zu den unter § 20a IfSG fallende Einrichtungen/Unternehmen stehen, in diesen aber, zum Beispiel als Handwerker, tätig sind, müssen den Nachweis nur gegenüber den genannten Leitungen erbringen.
  Delegationsmöglichkeiten werden im Folgenden behandelt.

- **Können die Leitungen der Einrichtungen/Unternehmen die Pflicht zur Entgegennahme des Nachweises auf andere Personen übertragen?**
  In der Praxis bestimmen die Leitungen der jeweiligen Einrichtungen/Unternehmen oftmals intern Beschäftigte, zum Beispiel aus der Personalabteilung, denen der Nachweis vorzulegen ist. Dies ist grundsätzlich datenschutzrechtlich möglich (siehe auch § 2 Nummer 15a Buchstabe a und § 2 Nummer 15b Buchstabe a IfSG; Deutscher Bundestag, Drucksache 20/250, Seite 60). An dieser Stelle muss allerdings insbesondere darauf geachtet werden, dass die Nachweise tatsächlich nur von den hierfür bestimmten Beschäftigten eingesehen werden und diese auf ihre Verschwiegenheitspflicht hingewiesen werden.
  Darüber hinaus kann die Leitung der in § 20a IfSG genannten Einrichtungen/Unternehmen die Entgegennahme des Nachweises alternativ an geeignete Dritte, wie zum Beispiel externe Personalverwaltungen, delegieren. Zu diesem Zweck müssten sie mit diesen einen Auftragsverarbeitungsvertrag schließen beziehungsweise einen bereits mit diesen geschlossenen Auftragsverarbeitungsvertrag gegebenenfalls aktualisieren, Artikel 28 DS-GVO.
- **Datenschutzkonformer Umgang mit dem Nachweis**
  Die genannten Personen müssen den Nachweis nur vorlegen. Das bedeutet, in den Nachweis darf zunächst nur Einsicht genommen werden. Dieser Nachweis darf daraufhin geprüft werden, ob er den oben genannten gesetzlichen Bestimmungen entspricht.
  Bei allen in den Einrichtungen/Unternehmen tätigen Personen darf nur jeweils notiert werden, dass ein Nachweis entsprechend § 20a IfSG vorgelegt worden ist und gegebenenfalls das Ablauf-/Enddatum dieses Nachweises, zum Beispiel bei den Genesenennachweisen sowie digitalen Impfnachweisen oder auch den Nachweisen über eine temporäre Kontraindikation. Darüber hinaus sieht das Gesetz in § 22a Absatz 1 IfSG bei bestimmten Impfnachweisen als Ablaufdatum den 30. September 2022 vor, zum Beispiel bei Personen bei denen nur zwei Einzelimpfungen nachweislich vorliegen. Auch dieses Ablaufdatum darf notiert werden. Denn nach Ablauf des jeweiligen Nachweises, muss ein dann gültiger Nachweis vorgelegt werden. Sofern dies nicht binnen Monatsfrist erfolgt, haben die Leitungen der in § 20a IfSG genannten Einrichtungen/Unternehmen dies an das jeweils für sie zuständige Gesundheitsamt zu melden und die personenbezogenen Daten der

betroffenen Person an dieses zu übermitteln, § 20a Absatz 4 IfSG. Der vorgelegte Nachweis darf nicht kopiert oder eingescannt und aufbewahrt werden.

Bei Personen, die keine unmittelbaren Beschäftigten der genannten Einrichtungen/Unternehmen sind, dürfen darüber hinaus natürlich auch der Vor- und Zuname und deren Kontaktdaten erhoben werden.

Mangels Erforderlichkeit dürfen weitere Daten wie zum Beispiel Impfmittel, das Datum der einzelnen Impfung usw. nicht notiert werden.

- **Wie oft muss der Nachweis vorgelegt werden?**
  Personen, die bereits in den genannten Einrichtungen tätig sind, mussten den Nachweis einmalig bis zum 15. März 2022 vorlegen. Hat der Nachweis ein Ablauf-/Enddatum, siehe oben, muss nach dessen Ablauf ein aktueller Nachweis ebenso einmalig vorgelegt werden und zwar innerhalb eines Monats nach Ablauf der Gültigkeit des bisherigen Nachweises, § 20a Absatz 4 Satz 1 IfSG. Die Leitung der unter § 20a IfSG fallenden Einrichtungen und Unternehmen dürfen die betroffenen Personen vor Ablauf der eben genannten Monatsfrist auffordern, den jeweiligen Nachweis vorzulegen. Die betroffenen Personen müssen aber vor Fristende der Aufforderung nicht nachkommen.

  Personen, die erst nach dem 15. März 2022 ihre Tätigkeit aufnehmen, haben den Leitungen der genannten Einrichtungen/Unternehmen oder den von diesen bestimmten Personen vor Aufnahme ihrer Tätigkeit den Nachweis vorzulegen.
- **Was passiert wenn ein Nachweis nicht fristgerecht vorgelegt wird oder aber Zweifel an der Gültigkeit eines Nachweises bestehen?**
  - **Personen, die bereits in den Einrichtungen/Unternehmen tätig sind:**
    Die Leitungen der genannten Einrichtungen/Unternehmen oder von diesen hierfür bestimmte Personen müssen unverzüglich das für die Einrichtung/das Unternehmen zuständige Gesundheitsamt informieren und dürfen zu diesem Zweck personenbezogene Daten der Person, die keinen Nachweis vorgelegt hat oder aber bei der Zweifel an der Echtheit oder inhaltlichen Richtigkeit ihres Nachweises bestehen, an dieses übermitteln, § 20a Absatz 2 Satz 2 IfSG.

In diesem Zusammenhang dürfen auf der Grundlage des § 20a IfSG neben dem Übermittlungsanlass (Nichtvorlage/Echtheits- oder Richtigkeitszweifel) personenbezogene Daten höchstens im Umfang des § 2 Nummer 16 IfSG (insbesondere Vor- und Zuname, Kontaktdaten) an das Gesundheitsamt übermittelt werden. Der Grundsatz der „Datenminimierung“ (Artikel 5 Absatz 1 Buchstabe c DS-GVO) ist zu beachten.

Darüber hinaus besteht auf der Basis einer Einwilligung die Möglichkeit, Informationen über bereits vereinbarte Impftermine durch die Einrichtungen/Unternehmen zu erheben und an das zuständige Gesundheitsamt weiterzuleiten, sofern sich dies im weiteren Verfahren zugunsten der betroffenen Personen auswirken kann. Die weiteren Voraussetzungen für die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten aufgrund einer Einwilligung sind stets zu beachten.

Auf Anforderung des zuständigen Gesundheitsamtes haben diese Personen den jeweiligen Nachweis diesem vorzulegen, § 20a Absatz 5 Satz 1 IfSG. Bei Zweifeln an der Echtheit oder inhaltlichen Richtigkeit eines Nachweises kann das zuständige Gesundheitsamt eine Untersuchung der betroffenen Person anordnen, ob eine medizinische Kontraindikation betreffend die Impfung gegen das Coronavirus SARS-CoV-2 vorliegt, § 20a Absatz 5 Satz 2 IfSG. Legt die betreffende Person dem Gesundheitsamt ihren Nachweis nicht vor oder leistet gegebenenfalls einer Anordnung einer ärztlichen Untersuchung nicht Folge, kann das Gesundheitsamt der betreffenden Person das Betreten der Einrichtung/des Unternehmens oder das Tätigwerden in dieser/diesem untersagen, § 20a Absatz 5 Satz 3 IfSG.

- **Personen, die in den Einrichtungen/Unternehmen nach dem 15. März 2022 tätig sein sollen:**

  Legen Personen, die nach dem 15. März 2022 in einer Einrichtung/einem Unternehmen tätig werden sollen, vor Beginn ihrer Tätigkeit keinen Nachweis vor, dürfen sie in der Einrichtung/dem Unternehmen nicht tätig werden, § 20a Absatz 3 Satz 4 IfSG.

  Bestehen Zweifel an der Gültigkeit des Nachweises ist seitens der Leitungen der Einrichtungen/Unternehmen wie oben dargestellt zu verfahren.

- **Meldepflicht der Pflegeeinrichtungen über den prozentualen Anteil geimpfter Personen (Impfquoten) an das Robert-Koch-Institut (RKI)**
  § 20a Absatz 7 Satz 1 IfSG enthält eine weitere gesetzliche Meldepflicht: Es sind monatlich Impfquoten an das RKI zu melden.
  - **Für wen gilt diese Meldepflicht?**
    Nicht alle in § 20a IfSG benannten Einrichtungen/Unternehmen sind zur Meldung von Impfquoten an das RKI verpflichtet. Vielmehr gilt diese Meldepflicht nur für die voll- oder teilstationäre Einrichtungen zur Betreuung und Unterbringung älterer, behinderter oder pflegebedürftiger Menschen oder vergleichbare Einrichtungen, die zugelassene Pflegeeinrichtungen im Sinne des § 72 des Elften Buches Sozialgesetzbuchs sind.
  - **Ausnahme von der Meldepflicht**
    Bevor die Leitungen der genannten Einrichtungen Daten für die Erfüllung der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG verarbeiten, sollte geprüft werden, ob für die Einrichtung eine Ausnahme von der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG vorliegt. Denn wenn die nachfolgenden Voraussetzungen erfüllt sind, entfällt die Meldepflicht, § 20a Absatz 7 Satz 5 IfSG:
    - Es gibt **landesrechtliche Meldeverfahren**, die bereits vor/am 19. März 2022 bestanden und
    - auf Bundesrecht beruhen und
    - die zu den durch das RKI zu erhebenden Daten über die Impfquoten anschlussfähig sind und
    - die Bundesländer nach Kreisen und kreisfreien Städten aufgeschlüsselte Daten direkt an das RKI übermitteln.

    Zur Feststellung, ob Sie von der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG befreit sind, wenden Sie sich in Zweifelsfällen an die für die Anwendung des Infektionsschutzgesetz für Sie zuständige jeweilige öffentliche Stelle.
  - **Welche Daten dürfen zur Erfüllung der Meldepflicht wie verarbeitet werden?**
    Wenn keine Ausnahme von der Meldepflicht vorliegt, müssen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen an das RKI folgende Impfquoten übermitteln:

Anteil der Personen, die gegen das Coronavirus SARS-CoV-2 geimpft sind, jeweils bezogen auf die Personen,

- die in der Einrichtung beschäftigt sind,
- behandelt, betreut oder gepflegt werden oder
- untergebracht sind.

In § 20a Absatz 7 Satz 1 IfSG ist ausdrücklich geregelt, dass an das RKI Daten nur in anonymisierter Form übermittelt werden dürfen.

Um die Meldepflicht gegenüber dem RKI zu erfüllen, dürfen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen den jeweiligen Impfstatus der

- Beschäftigten oder,
- Behandelten, Betreuten, Gepflegten oder
- Untergebrachten

verarbeiten.

Diesbezüglich dürfen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen zur Erfüllung ihrer Meldepflicht den jeweiligen Impfstatus ihrer Beschäftigten, Behandelten, Betreuten, Gepflegten oder Untergebrachten bei diesen abfragen und für den Zweck „Erfüllung der Meldepflicht gegenüber dem RKI“ speichern, § 20a Absatz 7 Satz 2 IfSG.

- **Beurteilung der Gefährdungslage anhand von Impfdaten**
  Besteht eine Meldepflicht und werden für deren Erfüllung bereits Impfdaten nach § 20a Absatz 7 Satz 2 verarbeitet, dürfen diese – soweit erforderlich – durch die Leitungen der in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen zur Beurteilung der Gefährdungslage in der Einrichtung im Hinblick auf die Coronavirus-Krankheit-2019 (COVID-19) verarbeitet werden, § 20a Absatz 7 Satz 3 IfSG.
- **Technische und Organisatorische Maßnahmen**
  Die Einrichtungen gemäß § 20a Absatz 7 Satz 1 IfSG müssen bei der Verarbeitung der Impfdaten für die Erfüllung ihrer Meldepflicht sowie für ihre Beurteilung der Gefährdungslage in der Einrichtung im Hinblick auf COVID-19 angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen treffen, § 20a Absatz 7 Satz 4 IfSG in Verbindung mit § 22 Absatz 2 BDSG.

- **Wann sind die Daten spätestens zu löschen?**
  Grundsätzlich haben die Leiterinnen und Leiter der genannten Einrichtungen/Unternehmen beziehungsweise deren Auftragsverarbeiter alle Daten zu löschen, wenn der Zweck für die Verarbeitung der personenbezogenen Daten entfällt, Artikel 17 Absatz 1 Buchstabe a DS-GVO.
  Unabhängig von einer Löschpflicht nach Artikel 17 Absatz 1 Buchstabe a DS-GVO sieht § 20a Absatz 7 Satz 7 IfSG für die im Zusammenhang mit der Meldepflicht und Beurteilung der Gefährdungslage anhand von Impfquoten verarbeiteten Daten vor, dass diese spätestens am Ende des sechsten Monats nach ihrer Erhebung gelöscht werden müssen. Jedenfalls muss eine Löschung aller auf Grundlage des § 20a IfSG verarbeiteten Daten spätestens mit Ablauf der Rechtsgrundlage am 31. Dezember 2022 erfolgen.

4.8 Festlegung der DSK

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 24. November 2022

1. Die DSK nimmt den Bericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“ und dessen Zusammenfassung zur Kenntnis.
2. Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann.
   Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.
3. Für eine vertiefte Bewertung der Gesprächsergebnisse stellt die DSK die beigefügte Zusammenfassung der Arbeitsgruppenergebnisse zur Verfügung.

Anlagen: Zusammenfassung des Berichts der Arbeitsgruppe

4.9 AG DSK „Microsoft-Onlinedienste“

Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung,

1. Untersuchungsauftrag, Verfahren und Untersuchungsgegenstand
Die DSK hatte am 22. September 2020 eine **Bewertung des Arbeitskreises Verwaltung** zu den dem Einsatz des Cloud-Dienstes Microsoft Office 365 (jetzt: Microsoft365) zu Grunde liegenden Online Service Terms (OST) sowie den Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die damalige Bewertung des AK Verwaltung kommt zum Ergebnis, *„dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“* sei.
Die DSK hat in ihrer Sitzung am 22. September 2020 eine Arbeitsgruppe unter Federführung Brandenburgs und des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gebeten, Gespräche mit Microsoft aufzunehmen, *„um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen.“*[8]
Daraufhin hat eine Arbeitsgruppe Ende 2020 Gespräche mit Microsoft begonnen. Teilnehmer der AG waren: Brandenburg und BayLDA (beide Leitung), BfDI, Baden-Württemberg, Berlin, Hessen, Mecklenburg-Vorpommern, Sachsen, Saarland und Schleswig-Holstein. Für Microsoft haben Beschäftigte der Microsoft Deutschland GmbH einschließlich eines Mitgliedes der Geschäftsleitung sowie je nach Schwerpunkt Ansprechpartner der Microsoft Corporation (USA) teilgenommen. Im Rahmen der Gespräche fanden 14 mehrstündige Videokonferenzen statt.
Bei den Gesprächen war zu berücksichtigen, dass federführende Datenschutzaufsichtsbehörde für Microsoft Ireland Operations, Ltd. als Partei des Auftragsverarbeitungsvertrags die irische Aufsichtsbehörde

[8] Vgl. TOP 9 („TOP 9 – Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365“), S. 5, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf.

ist und die deutschen Aufsichtsbehörden für die Aufsicht der jeweiligen deutschen Kunden (z. B. Unternehmen, Behörden, also die Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO) zuständig sind. Wesentliche Frage für die deutschen Aufsichtsbehörden war daher, ob die einzelnen Verarbeitungstätigkeiten der hiesigen Verantwortlichen (für die diese den Auftragsverarbeiter Microsoft beauftragt haben) rechtmäßig sind und ob der Auftragsverarbeitungsvertrag die Anforderungen von Art. 28 DS-GVO erfüllt. Zudem war zu berücksichtigen, dass der Cloud-Dienst Microsoft 365 in verschiedenen Funktionsumfängen, Varianten und Konfigurationen genutzt werden kann.

Grundlage der nachfolgenden Bewertungen ist der „Datenschutznachtrag zu den Produkten und Services von Microsoft“ (im Folgenden: „Datenschutznachtrag“) einschließlich der aktuellen Fassung vom 15. September 2022. Die Bewertung beruht auf der zum Abschluss des Berichts am 10. Oktober 2022 bestehenden Sach- und Rechtslage.

Der Bericht der Arbeitsgruppe enthält

a) eine alleine auf ausgewählte rechtliche Anforderungen der DSGVO beschränkte Bewertung, jedoch keine vollständige datenschutzrechtliche Bewertung des Cloud-Dienstes Microsoft 365,
b) im Wesentlichen eine Untersuchung, die sich auf die der sechs vom AK Verwaltung 2020 festgestellten vertraglichen Mängel beschränkt und keine darüber hinausgehenden Prüfungen enthält,
c) keine eigenständigen technischen Untersuchungen durch die Arbeitsgruppe und damit keine Prüfung der tatsächlich stattfindenden Datenflüsse und Verarbeitungen,
d) keine Untersuchung der Umsetzung der vertraglich festgelegten Verarbeitungen bzw. der tatsächlich stattfindenden Verarbeitungen,
e) keine Prüfung der Einzelkomponenten des Cloud-Dienstes, insbesondere keine Prüfung einzelner Funktionalitäten auf ihre Datenschutzkonformität (z. B. im Bereich Beschäftigtendatenschutz und Überwachung der Mitarbeitenden durch Verantwortliche),
f) keine Prüfung der einzelnen Verarbeitungstätigkeiten,
g) keine Prüfung des gesamten einschlägigen Vertragswerks von Microsoft sowie

h) keine Prüfung der datenschutzrechtlichen Anforderungen aus dem TTDSG und der Fragen, die sich aus dem Telekommunikationsrecht und des Fernmeldegeheimnisses ergeben.

Damit bietet der Bericht keine abschließenden Untersuchungen und kann anderweitige aufsichtliche Feststellungen weder ausschließen noch diesen vorgreifen. Dies gilt insbesondere im Hinblick auf bereits von einzelnen Aufsichtsbehörden durchgeführte Untersuchungen, die teils selbständige Mängel auflisten.[9]
Die Arbeitsgruppe hat Microsoft vor dem Abschluss ihres Berichts Gelegenheit zur Stellungnahme gegeben, diese Rückmeldungen geprüft und in ihren abschließenden Bewertungen berücksichtigt.
Die folgende Zusammenfassung bietet einen Überblick über wesentliche Ergebnisse der Gespräche und die dabei gegenüber den dem Auftrag der Arbeitsgruppe zu Grunde liegenden Prüfpunkten des AK Verwaltung erreichten bzw. nicht erreichten Nachbesserungen.

2. Wesentliche Ergebnisse

Microsoft hat im September 2022 einen aktualisierten *„Datenschutznachtrag zu den Produkten und Services von Microsoft“* (Englisch: *„Microsoft Products and Services Data Protection Addendum (DPA)“*) vorgestellt. Diese neue Version bringt vor allem Änderungen im Bereich der vertraglichen Formulierung der Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime Geschäftszwecke“ mit sich, kann als Ergebnis der Gespräche gesehen werden und adressiert damit einen Teil der Kritikpunkte des AK Verwaltung. Insgesamt konnte die Arbeitsgruppe in den vom AK Verwaltung benannten Kritikpunkten nur geringfügige Verbesserungen erreichen.
Zentrale und wiederkehrende Fragestellung der Gesprächsreihe war es, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als Verantwortlicher. Dies konnte nicht abschließend geklärt werden.

[9] Vgl. z.B. seitens der deutschen Aufsichtsbehörden: LfDI BW, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/ms-365 -schulen -hinweise-weiteres-vorgehen/#zusammenfassung ; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, Version 2.0 vom 18. Februar2021, S. 20 ff., https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf .

Verantwortliche müssen jederzeit in der Lage sein, **ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO** nachzukommen. Beim Einsatz von Microsoft 365 lassen sich hierbei auf Grundlage des „Datenschutznachtrags“ weiterhin Schwierigkeiten erwarten, da Microsoft nicht vollumfänglich offenlegt, **welche Verarbeitungen im Einzelnen stattfinden**. Zudem legt Microsoft weder vollständig dar, welche Verarbeitungen im Auftrag des Kunden noch welche zu eigenen Zwecken stattfinden. **Die Vertragsunterlagen sind in der Hinsicht nicht präzise** und erlauben im Ergebnis nicht abschließend bewertbare, ggf. sogar umfangreiche Verarbeitungen auch zu eigenen Zwecken.
Eine Verwendung personenbezogener Daten der Nutzenden (z. B. Mitarbeitenden oder Schüler:innen) zu eigenen Zwecken des Anbieters schließt den Einsatz eines Auftragsverarbeiters im öffentlichen Bereich (insbesondere an Schulen) aus. Die Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).
Aufgrund der Schwierigkeit für Verantwortliche des öffentlichen Bereichs, ihrer Rechenschaftspflicht nachzukommen, ist auch Art. 6 Abs. 1 lit. e DS-GVO i.V.m. jeweiligem Spezialrecht als Rechtsgrundlage schwer begründbar.

3. Zusammenfassung der erreichten Nachbesserungen im Einzelnen

Im Folgenden werden die nach dem Auftrag der DSK erzielten Nachbesserungen an den Kritikpunkten des AK Verwaltung zusammengefasst.

3.1. Festlegung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten

Die Arbeitsgruppe konnte im Rahmen der Gespräche mit Microsoft **keine signifikanten Nachbesserungen** in der Vertragsgestaltung hinsichtlich der Festlegung von Arten und Zwecken der Verarbeitung sowie der Arten der verarbeiteten personenbezogenen Daten erreichen. Es bleiben Nachbesserungen erforderlich, die den Gegenstand der Auftragsverarbeitung nicht nur umfassend, sondern auch spezifisch und so detailliert als möglich beschreiben sollten.
Dies könnte etwa durch eine kundenspezifische Konkretisierung nach dem Vorbild des Anhangs II der Standardvertragsklauseln der Kommission gemäß Art. 28 Abs. 7 DS-GVO erreicht werden. Möglich

wäre auch, Verweise auf ein formgerecht in den Vertrag einzubeziehendes und hinreichend detailliertes Verzeichnis der Verarbeitungstätigkeiten (VVT) des Verantwortlichen vorzusehen.

3.2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung „für legitime Geschäftszwecke“ (jetzt: „Geschäftstätigkeiten“)

Zum Themenkomplex der eigenen Verantwortlichkeit Microsofts im Rahmen der Verarbeitungen „für legitime Geschäftszwecke“ konnte die Arbeitsgruppe zwar Änderungen der vertraglichen Ausgestaltung erreichen. Ungeachtet unterschiedlicher Beurteilungen der datenschutzkonformen Ausgestaltung von Verarbeitungen vertragsgegenständlicher Daten zu eigenen Zwecken des Auftragsverarbeiters durch die europäischen Aufsichtsbehörden bewirken diese Vertragsänderungen jedoch aus Sicht der Arbeitsgruppe keine **substantiellen Verbesserungen**: Der „Datenschutznachtrag“ vom September 2022 enthält als Konsequenz der Gespräche mit der Arbeitsgruppe einen begrifflich veränderten Abschnitt über Datenverarbeitungen, die Geschäftstätigkeiten Microsofts dienen sollen, der erste Ansätze zur Eingrenzung und Konkretisierung zeigt. Allerdings hat Microsoft nach eigener Aussage **keine Anpassungen an den tatsächlichen Verarbeitungen** vorgenommen.

Eine genauere Untersuchung der vertraglichen Umgestaltung zeigt aus Sicht der Arbeitsgruppe, dass Microsoft die Grundansätze des bisherigen Regelungsmodells fortführt, sich für bestimmte Verarbeitungen **unzureichend eingegrenzte Rechte zu wenig konkretisierten Verarbeitungen** der verarbeiteten personenbezogenen Daten einräumen zu lassen. Es bleibt **weiterhin unklar**, welche personenbezogenen Daten im Rahmen der von Microsoft so genannten „legitimen“ Geschäftszwecke bzw. nun „Geschäftstätigkeiten“ verarbeitet werden.

Ebenso ist unklar, auf welcher Rechtsgrundlage die Überführung der im Auftrag verarbeiteten personenbezogenen Daten in die Verantwortlichkeit von Microsoft für die anschließende Verarbeitung zu Zwecken Microsofts samt der damit verbundenen umfassenden Nachweispflichten stattfindet. Ähnliches gilt für Daten wie **Telemetrie- und Diagnosedaten**, die Microsoft nach Kenntnis der Arbeitsgruppe in großem Umfang und grundsätzlich für eigennützige Zwecke erhebt. Besondere Schwierigkeiten bestehen dabei für öffentliche Stellen, da diese nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f) DSGVO zurückgreifen können.

3.3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, CLOUD Act, FISA 702

Der aktuelle Datenschutznachtrag vom September 2022 enthält **Veränderungen der bisherigen Bestimmungen**, die die Offenlegung von Microsoft als Auftragsverarbeiter bereitgestellten Daten im Rahmen eigener Geschäftszwecke „zur Erfüllung rechtlicher Verpflichtungen“ regeln. Dabei enthalten die Änderungen zwar neue Formulierungen, im Ergebnis bleiben die Befugnisse aber ähnlich umfangreich. Mit der Regelung wird etwa das Weisungsrecht des Kunden in Bezug auf Offenlegungen der im Auftrag verarbeiteten Daten eingeschränkt. Der Datenschutznachtrag erlaubt die Offenlegung, wenn diese rechtlich vorgeschrieben oder im „Datenschutznachtrag“ beschrieben sind. Solche Offenlegungen sind nicht auf Weisungen des Verantwortlichen beschränkt, sodass sie vor dem Hintergrund des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe a) DSGVO nur zulässig sind, wenn sie sich auf Verpflichtungen aus dem Unions- oder mitgliedstaatlichen Recht, dem Microsoft unterliegt, beschränken. Dies ist nicht der Fall. Damit genügt die Weisungsbindung Microsofts nicht den gesetzlichen Mindestanforderungen gemäß Art. 28 Abs. 3 UAbs. 1 S. 2 Buchstabe a DSGVO.

Aus den Untersuchungen der Arbeitsgruppe ergibt sich, dass sich Microsoft auch weit reichende Offenlegungen vertraglich vorbehält, die **im Falle ihrer Umsetzung nicht den in Art. 48 DSGVO aufgestellten Anforderungen entsprechen** würden.

3.4. Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO

Die ab 15. September 2022 geltende Version des „Datenschutznachtrags“ enthält gegenüber der vom AK Verwaltung geprüften Version **Ergänzungen zu den technisch-organisatorischen Maßnahmen**. Für ausdrücklich beschränkte bestimmte Datenkategorien (nämlich Kundendaten in „Core- Onlinediensten“ und nunmehr auch „Professional Services-Daten“) bestehen Garantie- und Datensicherheitsmaßnahmen. Zudem hat Microsoft dargelegt, dass es Interessierten nach einer Anmeldung Zugang zur Website servicetrust.microsoft.com („Servicetrust Website“), unter der Informationen über die durchgeführten technisch-organisatorischen Maßnahmen eingesehen werden können, bietet.

Es bleiben Rechtsunsicherheiten, da die Garantien über „Sicherheitsmaßnahmen“ formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten, nämlich „Kundendaten in „Core-Onlinediensten“ und „Professional-Service-Daten“, erfassen.

3.5. Löschung und Rückgabe personenbezogener Daten

Microsoft hat der Arbeitsgruppe die einzelnen Löschprozesse erläutert. Die Erläuterungen zeigen mit Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der „Cyberabwehr“, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschfristen für personenbezogene Daten nicht verlängern sollten. Zudem haben sich im Zuge der Umgestaltung des „Datenschutznachtrags“ auch Änderungen in Bezug auf Löschung ergeben, die allerdings auch Unklarheiten und Widersprüche mit sich bringen.

Nach Bewertung der Arbeitsgruppe genügt die Ausgestaltung der Rückgabe- und Löschverpflichtung **nicht in jedem Fall den gesetzlichen Anforderungen** aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO. Verantwortliche können wegen der Unklarheit der Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.

3.6. Information über Unterauftragsverarbeiter

Die Arbeitsgruppe hat mehrfach, teils kontrovers mit Microsoft die Ausgestaltung der Kontrollrechte des Verantwortlichen bei Veränderungen der Unterauftragsverarbeitungsverhältnisse diskutiert. Microsoft konnte trotz anfänglicher Vorbehalte zu einer Umstellung des bisher als Hol-Schuld des Verantwortlichen ausgestalteten Verfahrens zu organisatorischen und vertraglichen Anpassungen bewogen werden. Dies hat zu einer bereits Ende März eingeführten **Neugestaltung des Unterrichtungsverfahrens** geführt, die im aktuellen „Datenschutznachtrag“ vom September 2022 zu einer Streichung des bisherigen „Hol-Schuld“-Verfahrens geführt hat.

Die Arbeitsgruppe versteht Art. 28 Abs. 2 DSGVO dahingehend, dass die Information des Verantwortlichen „über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter“ die konkret beabsichtigte Änderung enthalten muss und nicht nur den allgemeinen Hinweis, dass Änderungen geplant sind.

Das von Microsoft bereitgestellte Muster einer Benachrichtigungs-E-Mail enthält nur eine Information über geplante Änderungen, aber nicht die konkret geplanten Änderungen. Die der Arbeitsgruppe vorgestellte Liste über Unterauftragsverhältnisse unterscheidet zudem

bislang im Wesentlichen danach, für welchen Dienst bzw. welche Funktionalität Unterauftragnehmer eingesetzt sind und benennt deren Sitz und die ihnen zugänglichen Datenkategorien. Im Vergleich dazu sehen die von der EU-Kommission bereitgestellten Standardvertragsklauseln deutlich detailliertere Angaben über Name, Anschrift und Kontaktperson des Unterauftragsverarbeiters sowie eine Beschreibung der jeweiligen Verarbeitung vor, die eine klare Abgrenzung der Verantwortlichkeiten mehrerer eingesetzter Unterauftragsverarbeiter erlauben sollen.

3.7. Datenübermittlungen in Drittstaaten

Der „Datenschutznachtrag“ vom September 2022 enthält die Regelung, dass **der Kunde Microsoft „beauftragt (...), (...) personenbezogene Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind“**. Für sämtliche Übermittlungen von insbesondere personenbezogenen Daten gelten danach die von Microsoft implementierten Standardvertragsklauseln der EU-Kommission von 2021.

Die Gespräche der Arbeitsgruppe mit Microsoft bestätigten entsprechend den vertraglichen Regelungen, dass bei der Nutzung von Microsoft 365 personenbezogene Daten jedenfalls in die USA übermittelt werden. **Eine Nutzung von Microsoft 365 ohne Übermittlungen personenbezogener Daten in die USA sei nicht möglich**. Ab Dezember 2022 plane Microsoft, allen Kunden im EU-Raum anzubieten, Kundendaten, Supportdaten und sonstige personenbezogene Daten der Kunden grundsätzlich – d.h. nicht ausnahmslos, nicht etwa für bestimme IT-Sicherheitsmaßnahmen – im EU- Raum zu speichern und zu verarbeiten („EU Data Boundary“).

Für die USA hat der EuGH in „Schrems II“ festgestellt, dass FISA 702 und E.O. 12333 unverhältnismäßige Zugriffsrechte für US-Geheimdienste vorsehen und für EU-Bürger kein gerichtlicher Rechtsschutz gegeben ist. Um die vom EuGH identifizierten am EU-Maßstab gemessenen grundrechtlichen Unzulänglichkeiten von FISA 702 auszugleichen, wäre es erforderlich, Maßnahmen zu ergreifen, die den Zugriff der US-Behörden – und damit von Microsoft – auf personenbezogene Daten verhindern oder ineffektiv machen. Viele der in Microsoft 365 enthaltenen Dienste erfordern einen Zugriff von Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten. Die naheliegende Möglichkeit der **Verschlüsselung der verarbeiteten Daten ist regelmäßig nicht möglich**, beispielsweise wenn die Daten im

Browser angezeigt werden müssen. Microsoft hat somit regelmäßig und letztlich schon zur Erfüllung vertraglicher Leistungspflichten die Möglichkeit, Daten im Klartext zu lesen. Es handelt sich mithin um eine klassische Ausprägung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses. **Für diesen Anwendungsfall ist es den Aufsichtsbehörden bislang nicht gelungen, ergänzende Schutzmaßnahmen zu identifizieren, die zu einer Rechtmäßigkeit des Datenexports führen könnten.**

Die von Microsoft derzeit im Abschnitt „Ort der ruhenden Daten" vorgesehenen Maßnahmen für die Speicherung der Daten (data at rest) führen weder zum Ausschluss einer Übermittlung noch begründen sie hinreichende Schutzmaßnahmen. Für die weiteren Verarbeitungen (abseits der Speicherung) enthält der Abschnitt „Datenübermittlung und Ort" („Data Transfers and Location") keine Aussagen zur Datenlokalisierung. Auch die von Microsoft im „Nachtrag zu zusätzlichen Schutzmaßnahmen" zugesagten Maßnahmen sind nicht geeignet, die am Maßstab des EU- Rechts gemessenen grundrechtlichen Unzulänglichkeiten des US-amerikanischen Rechts auszugleichen. Zudem behält sich Microsoft vertraglich auch weit reichende Offenlegungen vor, die im Falle ihrer Umsetzung nicht den in Art. 48 DSGVO aufgestellten Anforderungen entsprechen würden.

Für Übermittlungen personenbezogener Daten in **andere Drittländer als die USA** fehlt es bereits an einer Bewertungsgrundlage.

Die von Microsoft bereits avisierte künftige verstärkte **Verlagerung der Datenverarbeitung in die EU erscheint vor diesem Hintergrund hilfreich**, ist in der Umsetzung aber auch vor dem Hintergrund etwaiger extraterritorial wirkender Rechtsvorschriften zu beobachten und zu bewerten.

Ob und in welchem Umfang durch die am 7. Oktober 2022 von US-Präsident Biden und Generalstaatsanwalt Garland vorgestellte Executive Order „Enhancing Safeguards for United States Signals Intelligence Activities" und begleitende Rechtsverordnungen des US-Justizministeriums Änderungen des für die Bewertung von Drittstaatentransfers maßgeblichen Bedingungen des US- Rechts eingetreten sind, bleibt angesichts noch ausstehender Vollzugsschritte zur Implementierung dieser Regelungen im Rahmen dieses Berichts unberücksichtigt.

4.10 Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
(Stand: Oktober 2022)

Der deutsche Gesetzgeber hat zur Umsetzung der europäischen Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DI-RL) in das Bürgerliche Gesetzbuch (BGB) neue Vorschriften zu Verbraucherverträgen über digitale Produkte aufgenommen. Diese sind am 1.1.2022 in Kraft getreten. In den neuen zivilrechtlichen Verbraucherschutzvorschriften über digitale Produkte wird in § 312 Abs. 1a BGB und § 327q BGB „Vertragsrechtliche Folgen datenschutzrechtlicher Erklärungen des Verbrauchers“ ein eindeutiger Bezug zum Datenschutzrecht hergestellt.

§ 312 Abs. 1a BGB lautet

„Die Vorschriften der Kapitel 1 und 2 dieses Untertitels sind auch auf Verbraucherverträge anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Dies gilt nicht, wenn der Unternehmer die vom Verbraucher bereitgestellten personenbezogenen Daten ausschließlich verarbeitet, um seine Leistungspflicht oder an ihn gestellte rechtliche Anforderungen zu erfüllen, und sie zu keinem anderen Zweck verarbeitet.“

Nunmehr wird in der Praxis stark diskutiert, welche datenschutzrechtlichen Auswirkungen diese Vorschriften auf das sog. Geschäftsmodell „Bezahlen mit Daten“ haben. Insbesondere im Internet wird dieses Geschäftsmodell seit langem praktiziert, wenn werthaltige Inhalte, wie z.B. Zeitungsartikel, oder Dienstleistungen, wie die Bereitstellung von Plattformen zur sozialen Vernetzung oder Suchmaschinen, von den Nutzer:innen nicht mit Geld bezahlt werden. Die vermeintlich kostenlosen Inhalte und Dienstleistungen werden regelmäßig über personalisierte Werbung finanziert. Zu diesem Zweck, wird das Verhalten der Nutzer:innen häufig nachverfolgt und die so gewonnenen Daten werden zu detaillierten Nutzerprofilen zusammengeführt und ausgewertet, um auf dieser Grundlage Werbung darzustellen und dadurch die Werbeeinnahmen zu generieren.

Die Verarbeitung personenbezogener Daten im Rahmen dieser Geschäftsmodelle muss auf eine der gesetzlichen Erlaubnistatbestände gemäß Art. 6 Abs. 1 Buchstabe a, b oder f DS-GVO gestützt werden können und auch den sonstigen Anforderungen der Datenschutz-Grundverordnung gerecht werden. Die neuen Verbraucherschutzvorschriften des BGB stellen keine eigene Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dar.
Die DSK beurteilt die datenschutzrechtlichen Auswirkungen der neuen Verbrauchervorschriften wie folgt:
1. Die §§ 327 ff. BGB sind nur anwendbar, wenn ein Vertrag über digitale Produkte geschlossen wurde.
Ob zwischen Nutzer:innen und Betreiber:innen einer Website, deren Angebote durch personalisierte Werbung (teilweise) finanziert werden, tatsächlich ein Vertrag über digitale Produkte zustande kommt, hängt insbesondere davon ab, inwiefern die Parteien den Willen haben, sich rechtlich zu binden. Eine verallgemeinernde Auslegung dahingehend, dass jeder Aufruf einer Webseite, deren Angebot die Verarbeitung personenbezogener Daten beinhaltet, oder jede Interaktion mit einem Einwilligungsbanner zum Abschluss eines Verbrauchervertrages führt, verbietet sich vor dem Hintergrund der Anforderungen der §§ 133, 157 BGB. Insbesondere kann allein die Bereitstellung der personenbezogenen Daten nicht als konkludente Willenserklärung der Betroffenen zum Abschluss eines Vertrages über digitale Produkte gewertet werden. In der Praxis wird es maßgeblich darauf ankommen, in jedem konkreten Fall zu untersuchen, ob zwei übereinstimmende Willenserklärungen mit entsprechendem Rechtsbindungswillen vorliegen. Nur in diesem Fall kommen die §§ 327 ff. BGB überhaupt zum Tragen.
2. Wurde zwischen dem Unternehmen und dem Verbraucher ein Vertrag über digitale Produkte geschlossen, ist jede Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem geschlossenen Vertrag nur rechtmäßig, wenn sie auf eine Rechtsgrundlage der Datenschutz- Grundverordnung gestützt werden kann.
Die zivilrechtlichen Vorschriften über den Verbrauchervertrag stellen keine eigene Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dar. Für die Datenverarbeitung im Rahmen des Verbrauchervertrages über digitale Inhalte kommen grundsätzlich Art. 6 Abs. 1 Buchstabe a, b und f DS-GVO in Betracht. Sofern besondere Kategorien personenbezogener Daten verarbeitet werden sollen, ist

zusätzlich Art. 9 DS-GVO zu berücksichtigen. Die Erwägungsgründe Nr. 37 und 38 DI-RL halten ausdrücklich fest, dass die DS-GVO von der Richtlinie unberührt bleibt und die Vorgaben der DS-GVO für alle personenbezogenen Daten gelten, die im Zusammenhang mit den von dieser Richtlinie erfassten Verträgen verarbeitet werden. Eine Verarbeitung personenbezogener Daten im Zusammenhang mit einem Vertrag, der in den Anwendungsbereich der Richtlinie fällt, ist daher nur rechtmäßig, wenn sie mit den Bestimmungen der DS-GVO im Einklang steht. Gleiches gilt für die neuen Verbraucherschutzvorschriften im BGB, die der Umsetzung der DI-RL dienen.

3. § 327q BGB trifft keine Aussage zu den Auswirkungen der zivilrechtlichen Verbraucherschutzvorschriften auf das Datenschutzrecht. Es werden nur umgekehrt die zivilrechtlichen Auswirkungen auf den Verbrauchervertrag festgelegt wenn Verbraucher von ihren datenschutzrechtlichen Rechten Gebrauch gemacht haben, eine Einwilligung zu widerrufen oder einer Datenverarbeitung, die auf Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt wird, gemäß Art. 21 DS- GVO zu widersprechen.

§ 327q BGB regelt die vertragsrechtlichen Folgen datenschutzrechtlicher Erklärungen des Verbrauchers. In Absatz 1 wird festgestellt, dass die Ausübung von datenschutzrechtlichen Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Im Falle des Widerrufs der von einem Verbraucher erteilten datenschutzrechtlichen Einwilligung oder des Widerspruchs gegen eine weitere Verarbeitung seiner personenbezogenen Daten wird dem Unternehmen unter den Voraussetzungen des § 327q Abs. 2 BGB ein außerordentliches Kündigungsrecht des Verbrauchervertrages zuerkannt. Absatz 3 stellt ergänzend klar, dass die Ausübung von Datenschutzrechten oder die Abgabe datenschutzrechtlicher Erklärungen durch den Verbraucher keine Ersatzansprüche des Unternehmers gegen diesen begründen können.

4. Die neuen Verbraucherschutzvorschriften im BGB haben keine Auswirkungen auf die Anwendung von § 25 TTDSG.

Wurde zwischen dem Unternehmen und dem Verbraucher ein Vertrag über digitale Produkte geschlossen, hat dies keine Auswirkungen auf die Anwendung § 25 TTDSG. Das Unternehmen muss prüfen, ob für Vorgänge der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, eine Einwilligung erforderlich oder

eine Ausnahme einschlägig ist. Wie oben geschildert, kommen die §§ 327 ff. BGB überhaupt erst zur Anwendung, wenn ein Verbrauchervertrag geschlossen wird. Die Qualitätsanforderungen, die § 327e BGB aufstellt, können den „objektiv geschuldeten Funktionsumfang“ eines Telemediendienstes mithin erst beeinflussen, wenn mit Nutzer:innen ein Vertrag über digitale Produkte zustande kommt. Selbst dann ist weiterhin im Einzelfall zu prüfen, ob die Vorgänge unbedingt erforderlich sind, um den von Nutzer:innen gewünschten Dienst (mangelfrei) zur Verfügung zu stellen. Weitere Ausführungen hierzu können der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (letzte Fassung vom 24. November 2022) entnommen werden.

5. Vorträge und Veranstaltungen

Lernen Schulung Training - Kostenloses Bild auf Pixabay

5.1 Vorträge und Veranstaltungen

Der TLfDI informiert! Der TLfDI ist unterwegs! – Höhepunkt im Berichtszeitraum war die Großveranstaltung „Digitalisierung der (Hoch-)Schulen!“ am 19. September 2022 im Augustinerkloster zu Erfurt. Der TLfDI und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) setzten zudem ihre Zusammenarbeit im Rahmen ihres Kooperationsvertrages mit der regelmäßigen virtuellen Vortragsreihe zum Thema „Datenschutz beim häuslichen Lernen“ fort. Auch die (unentgeltlichen) Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena zur „Einführung in das Datenschutzrecht“ standen den Studierenden wieder virtuell und im Wintersemester in Präsenz des TLfDI zur Verfügung. Teilnehmen konnten ab dem Wintersemester 2022 nun auch Studierende der Wirtschaftswissenschaften. Inzwischen können mit einer Klausur auch Creditpoints für das Examen erworben werden.

Großveranstaltung „Digitalisierung der (Hoch-)Schulen!“
140 Gäste, darunter vorwiegend Thüringer Schulleiter*innen, sowie Schüler*innen, Schüler- und Elternsprecher*innen und Journalisten, waren der Einladung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu seiner Tagung zur

„Digitalisierung der (Hoch-)Schulen“ im September 2022 ins Augustinerkloster zu Erfurt gefolgt. Denn unbarmherzig brachte es die Corona-Pandemie an den Tag: Schulen und Hochschulen leben in einer Welt, die mit den digitalen Realitäten zu wenig Berührungspunkte hat. Schüler*innen und Lehrer*innen können Smartphones und Tablets bestenfalls bedienen, wissen aber nicht, was diese Geräte sowie die heruntergeladenen Apps mit personenbezogenen Daten anrichten können und anrichten. Was passiert mit den Daten bei Videokonferenzen? Was passiert beim Unterricht mit den YouTube-Clips? Vor allem vor diesen Fallstricken beim Online-Unterricht wurde gewarnt. Verantwortlich für den Datenschutz im Unterricht sind im Freistaat Thüringen die Schulleiter*innen. Sie bestimmen, wie und wofür Daten verarbeitet werden. Unterricht am Laptop, Hausaufgaben in der Schulcloud, der TLfDI warnt immer wieder vor den Gefahren durch Tablets und Smartphones im Unterricht. Er schlägt bessere Ausbildung bereits im Studium und in Weiterbildungen, sowie neue Zuständigkeiten vor. Fazit: Für den TLfDI gibt es zwei Auswege aus diesem Problem: Entweder werden die Lehrerinnen und Lehrer so aus- und weitergebildet, dass sie für die datenschutzrechtlichen Aufgaben gewappnet sind oder die Verantwortung für den Datenschutz im Unterricht wird verlagert. Fortsetzung folgt!

Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena

Die Vorlesungen zur „Einführung in das Datenschutzrecht“ standen den Studierenden wieder virtuell und im Wintersemester in Präsenz des TLfDI zur Verfügung. Teilnehmen konnten ab dem Wintersemester 2022 nun auch Studierende der Wirtschaftswissenschaften und vor allem der Erziehungswissenschaften. Inzwischen können mit einer Klausur auch Creditpoints für das Examen erworben werden.

„Datenschutz beim häuslichen Lernen“

Fortgesetzt wurde durch das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) und die Behörde des TLfDI, in regelmäßigen Abständen, die Videokonferenzreihe zum Thema „Datenschutz beim häuslichen Lernen“, um vor allem die Schulleitungen zu erreichen. Mit diesem Format werden regelmäßig themenbezogene Frage- und Fortbildungsrunden zum Schwerpunkt Datenschutz angeboten. Fortsetzung folgt auch hier! Ausblick: Videokonferenzen mit der Landeselternvertretung und den Berufsschulleitungen durch beide Kooperationspartner.

Der TLfDI versorgte die Schulleitungen auch weiterhin kontinuierlich mit wichtigen Informationen zur Schulsoftware und dem Datenschutz beim häuslichen Lernen, während der Pandemie in Briefform und durch FAQs.

„Datenschutz geht zur Schule“ – ein neues Videoformat

Das gemeinsame Format sensibilisiert Schüler*innen dafür, mit eigenen Daten und den Daten anderer im Internet und in den sozialen Medien sicherer und bewusster umzugehen. Die vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. ins Leben gerufene Initiative „Datenschutz geht zur Schule“ sensibilisiert Schüler*innen in ganz Deutschland dafür, mit eigenen Daten und den Daten anderer im Internet und in den sozialen Medien sicherer und bewusster umzugehen. Das Sensibilisierungsangebot der ehrenamtlich tätigen Dozent*innen wurde in den letzten Jahren erfolgreich in den Schulen etabliert. Um auch in Pandemiezeiten ohne Schulbesuch passende Impulsvorträge liefern zu können, hat die Initiative „Datenschutz geht zur Schule“ mit freundlicher Unterstützung der Datenschutzaufsichtsbehörden LfDI Baden-Württemberg, des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA), des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(TLfDI) sowie des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) das Projekt „Datenschutz – leicht erklärt“ ins Leben gerufen. Hierbei wurden in 18 Einzelvideos die Datenschutz-Themen aufgezeichnet, die bisher nur in den Klassenräumen im Rahmen der Sensibilisierungsveranstaltungen vermittelt wurden.
Lesen Sie hier weiter: https://www.tlfdi.de/datenschutz/schule-1/links-fuer-lehrkraefte-und-schueler/

Link zum Film:
https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/schule/Datenschutz_leicht_erklaert/naheliegende_Themen/Drohne_720p_mit_UT.mp4

Ebenso beteiligte sich der TLfDI wieder als Referent auf verschiedenen Podien, so unter anderem auf der didacta 2022 und der Multivision e. V.
Ausblick für 2023: didacta 2023 in Stuttgart und Podium bei der Frankfurter Buchmesse.

Es gab weitere Vorträge beim Blindenverein, der IHK, dem Kinderhilfswerk, dem Bildungswerk ver.di, an Fachschulen und Schulämtern sowie bei den Landeselternsprechern. Ausblick: Geplant sind regelmäßige ViKos mit Berufsschulleitungen.

Seit November 2022 gibt es einen Runden Tisch mit der IHK Erfurt und Vertretern der Wirtschaft mit dem TLfDI.

Der TLfDI betreute auch wieder diverse Seminarfacharbeiten der Schüler*innen Thüringens.

News reporter or TV journalist at press conference, holding microphone and writing notes: © wellphoto

Die Presse- und Öffentlichkeitsarbeit beantwortete 29 Presseanfragen von Journalist:innen und Redaktionen. Der TLfDI gab diverse Interviews bei Funk und Fernsehen und veröffentlichte 14 Pressemitteilungen. Der TLfDI nahm erfolgreich am Tag der offenen Tür 2022 im Landtag teil.

Der TLfDI veröffentlichte weiterhin einen Beitrag zu Bildung und Schule in der BvD-News 3/2022 „Digitalisierung und Medienkompetenz – Wo klemmt‘s?“.
Lesen Sie hier: https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/schule/DIGITALISIERUNG_UND_MEDIENKOMPETENZ_WO_KLEMMT_S.pdf

Ausblick: TLfDI zum Anfassen (Nordhausen, Eisenach, Sondershausen, Altenburg) und Großveranstaltung zu „KI und Schule“ am 13. September 2023 im Augustinerkloster zu Erfurt ☺

Stichwortverzeichnis