TLfDI

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

2019

2. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

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, Telefax: +49 (361) 57-3112904 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
Redaktionsschluss:	31.05.2020

2. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019
Zitiervorschlag: 2. TB DS-GVO LfDI Thüringen

Der 2. Tätigkeitsbericht DS-GVO steht im Internet unter https://www.tlfdi.de/tlfdi/datenschutz/taetigkeitsberichte-zum-datenschutz/ zum Abruf bereit.

Erfurt, im Juni 2020

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort 8

1. Schwerpunkte im Berichtszeitraum 10

1.1 Schwerpunkte 10

1.2 Statistik 13

2. Themengebiete 17

2.1 „Es ist des Lernens kein Ende“ – Irrtümer über die DS-GVO 17

2.2 Die Hambacher Erklärung: ein erstes Rahmenwerk zur Regulierung von künstlicher Intelligenz 21

2.3 Die Datenschutzordnung für parlamentarische Aufgaben des Landtags und seiner Fraktionen und ihre Kontrolle – ohne den TLfDI 26

2.4 Der TLfDI vor Ort 29

2.5 Recht auf Kopie im Rahmen der Auskunftserteilung? 31

2.6 Datenschutz-Folgenabschätzung 34

2.7 Datensicherheitsmaßnahmen gemäß DS-GVO 36

2.8 EuGH-Urteil zu Gmail 38

2.9 Positionspapier zur biometrischen Analyse 41

2.10 Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung 42

2.11 Windows 10 44

2.12 Orientierungshilfe Telemedien 46

2.13 Facebook-Fanpage 47

2.14 Google-Formular 49

2.15 Auch über den Clouds gibt es keine Datenschutz-Freiheit 50

2.16 Meldungen nach Art. 33 – keine Angst vor Bußgeldern! 52

3. Fälle öffentlicher Bereich 54

3.1 Transparenz bei Online-Petitionen 54

3.2 Zentrales DMS 56

3.3 Alles richtig bei der Richtlinie zur Aufbewahrung von Akten und sonstigem Schriftgut in der Thüringer Verwaltung? 58

3.4 Das lange Warten auf Auskunft 60

3.5 „Wer sitzt da neben dir?“ – Blitzerfotos von Beifahrern 61

3.6 Transparenz von Gerichtsverhandlungen – Öffentlichkeitsgrundsatz vs. Datenschutz 63

3.7 Ein Identitätsnachweis ist nicht in jedem Fall ein Muss 65

3.8 Auskunftsrecht = Akteneinsichtsrecht beim Notar? 65

3.9 Datenschutz bleibt Datenschutz – mit oder ohne Regelung des Thüringer Gesetzgebers zum Kommunalwahlrecht 67

3.10 Adressen im Amtsblatt – rechtlich zulässig, aber datenschutzrechtlich fragwürdig 69

3.11 Auskunft ist nicht gleich Auskunft 70

3.12 Ratsinformationssysteme 72

3.13 Offenbarung von Bürgerdaten in der Kfz-Zulassungsstelle 75

3.14 Brisanter Prüfungsbericht des Thüringer Rechnungshofs ... 77

3.15 Nur fit ans Steuer – auch aus datenschutzrechtlicher Sicht erlaubt 79

3.16 Anwohnerparkplaketten während des Thüringentags 82

3.17 Hilfssheriff on Tour 83

3.18 Hundesteueranmeldung – „Ein Hund oder kein Hund?“ 85

3.19 Informationspflichten nach der DS-GVO im Bereich der Vollstreckungsabteilung 87

3.20 Datensicherheit beim Telefax 90

3.21 Was darf in Dienstplänen mitgeteilt werden? 92

3.22 Weitergabe von Fehlzeiten und Noten durch die Berufsschule jetzt geregelt 93

3.23 Mitarbeiterüberwachung: Gleiches mit Gleichem vergelten? 95
3.24 Beihilfe: Digitalisierung des Antragsverfahrens 98
3.25 DigitalPakt: Digitalstrategie des Thüringer Bildungsministeriums – Datenschutz ist mit im Boot 99
3.26 Die Schul-Cloud des Hasso-Plattner-Instituts steht in abgespeckter Form vor Einführung in Thüringer Pilotschulen 100
3.27 Liveübertragung des Unterrichts aus dem Klassenzimmer? 103
3.28 Automatisiertes Verfahren soll Schultagebuch für Kinder beruflich Reisender ersetzen 105
3.29 E-Mail-Adressen für Thüringer Lehrkräfte elektronisch kommunizieren – aber sicher! 107
3.30 Schuldaten auf dem Privat-PC eines Lehrers. Ist das zulässig? 109
3.31 Schule stellt teilweise sensible personenbezogene Daten von Schülern und Eltern ins Internet 110
3.32 Akteneinsicht oder Kopie der Akte? Was sagen Datenschutzgrundverordnung und das Verwaltungsverfahrensgesetz? 113
3.33 Kommunales Haushaltsrecht und Betriebskosten im Kindergarten: Keine Rechnungsprüfung ohne Daten 114
3.34 Forschungsprojekt „Sicherheit und Kriminalität in Deutschland“ (SKiD) 116
3.35 Der Personalausweis ist kein Pfandmittel 118
3.36 Datenschutz im digitalen Zeitalter: telemedizinische Versorgung von Schlaganfallpatienten 119
3.37 Wie sicher ist „die Neue“? 122
3.38 E-Mail für dich: aus Mexiko vom Klinikum 124
3.39 Informationspflicht nach Art. 13 und 14 DS-GVO 127
3.40 „Bankengeheimnis ade?“ 130

3.41 Übermittlung von Steuerdaten: Ausland oder Zeitzone? ..132

3.42 Können im Vorhinein angekreuzte Felder eine Einwilligung sein? 133

4. Fälle nicht-öffentlicher Bereich 135

4.1 Datenschutzbeauftragter als IT-Sicherheitsbeauftragter – bestehen Interessenkonflikte? 135

4.2 Anwaltswerbung mit Daten Dritter 137

4.3 Datenschleuder im Internetportal für Immobilien 139

4.4 Datenverarbeitung im Rahmen einer Wohnungseigentümergemeinschaft 141

4.5 Gefrorener Datenschutz – Eiscafé totalüberwacht 143

4.6 Die Tücken bei Bewerbungen per E-Mail 146

4.7 Einwilligung im Postkartenformat 148

4.8 Welche Daten seiner Arbeitnehmer darf ein Arbeitgeber ans Thüringer Landesamt für Statistik übermitteln? 151

4.9 GPS-Überwachung im Dienstfahrzeug 154

4.10 Dürfen Recyclingunternehmen Personalausweiskopien anfertigen? 156

4.11 Gefahr erkannt beim Faxversand 159

4.12 Veröffentlichung von Vereinsprotokollen in Schaukästen 160

4.13 Antrag auf Auskunftserteilung nur gegen Kostenübernahme? 162

4.14 Dürfen Berufsgeheimnisträger Daten per E-Mail senden? 164

4.15 Müssen nach einer Kündigung die Gemeinschaftsbilder entfernt werden? 167

4.16 Datenschutz am Tresenbereich einer Arztpraxis 168

4.17 Das Haushaltsprivileg – keine Anwendung der DS-GVO im ausschließlich persönlichen und familiären Bereich 169

4.18 Keine familiären Tätigkeiten trotz Verwandtschaftsverhältnis 172

4.19 Unterhaltsvorschussantrag – welche Daten des nicht mit den Kindern lebenden Elternteils dürfen ans Jugendamt weitergegeben werden? 175

4.20 Sind Ortschroniken nach Inkrafttreten der DS-GVO noch zulässig? 179

4.21 Augen auf bei der Rechtsanwendung – Unrechtmäßige Mandantenakquise einer Rechtsanwaltskanzlei aufgrund rechtmäßig erhaltener Gerichtsakten 182

5. Entschließungen und Beschlüsse 184

5.1 Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! 184

5.2 Hambacher Erklärung zur Künstlichen Intelligenz 186

5.3 Keine Abschaffung der Datenschutzbeauftragten 192

5.4 Digitalisierung der Verwaltung – datenschutzkonform und bürgerfreundlich gestalten! 193

5.5 Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen 196

5.6 Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten 198

5.7 Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte! 200

5.8 Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke! 203

5.9 Informationen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden zu Datenübermittlungen aus Deutschland in das Vereinigte Königreich Großbritannien und Nordirland ab dem 30. März 2019 205

5.10 Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit 208

5.11 Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10 210

5.12 Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO 212

5.13 Beschluss: Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen 215

5.14 Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU 218

5.15 Asset Deal – Katalog von Fallgruppen 221

5.16 Spezifische Aufsichtsbehörden 223

5.17 Datenschutzrechtliche Verantwortlichkeit innerhalb der Telematik-Infrastruktur 225

5.18 Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste 226

5.19 Verhaltensbasierte Werbung 227

5.20 Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO 229

6. Abschlussbericht des Untersuchungsausschusses zum Vorgehen des TLfDI im Fall des Aktenlagers in Immelborn 258

7. Vorträge und Veranstaltungen 265

7.1 Der TLfDI informiert! Der TLfDI ist unterwegs! – Presseanfragen zur DS-GVO und Einladungen zu Vorträgen und Veranstaltungen reißen auch 2019 nicht ab! 265

Stichwortverzeichnis 270

Vorwort

Dr. Lutz Haase

Ab diesem Jahr erwartet Sie nun, so wie es die Datenschutz-Grundverordnung (DS-GVO) vorsieht, jährlich der Bericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über sein Tätigwerden als Aufsichtsbehörde nach DS-GVO. Der Berichtszeitraum ist zwar kürzer, die Themen und Aufgabenstellung, mit denen der TLfDI sich beschäftigt hat, nehmen aber an Vielfältigkeit zu.
Das Jahr war für die Verantwortlichen dadurch geprägt, bei der Anwendung des seit 25. Mai 2018 (Wirksamwerden der DS-GVO) neu geltenden Rechts Fuß zu fassen. Nach wie vor haben den TLfDI sehr viele Beratungsanfragen erreicht, es waren aber auch etliche Beschwerden zu verzeichnen. Der TLfDI hat viele Verantwortliche dabei begleitet, die neuen Instrumente der DS-GVO wie die Datenschutzfolgenabschätzung, das Verzeichnis über Verarbeitungstätigkeiten sowie die Regelungen zur gemeinsamen Verantwortlichkeit und Auftragsverarbeitung in der Praxis umzusetzen. Dabei ist die Behörde auch in diesem Jahr an die Grenzen ihrer Leistungsfähigkeit geraten.
Ich möchte meinen Mitarbeitern an dieser Stelle ausdrücklich für ihren unermüdlichen Einsatz in Sachen Datenschutz in diesem Jahr danken und freue mich sehr darüber, dass die große Anzahl der Aufgaben auch im Jahr 2020 angegangen werden kann. Die Aufgaben der DS-GVO als Aufsichtsbehörde können vom TLfDI nur umgesetzt werden, wenn ihm weiterhin ausreichend Personal zur Verfügung gestellt

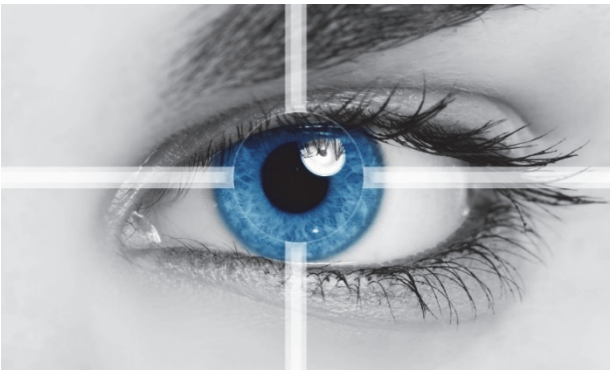
wird. Dies zu erreichen wird auch im folgenden Jahr einer meiner wichtigen Vorsätze bleiben, denn es gilt das stark gefährdete Grundrecht der informationellen Selbstbestimmung zu schützen – es gibt also viel zu tun!

Ich wünsche Ihnen viel Spaß und nützliche Erkenntnisse beim Lesen des Berichts über die Aktivitäten der Behörde im Jahr 2019.

Ihr

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

1. Schwerpunkte im Berichtszeitraum



© Minerva Studio - Eye close-up - fotolia.com

1.1 Schwerpunkte

Auch das Jahr nach dem Wirksamwerden der Datenschutz-Grundverordnung stand beim TLfDI ganz im Zeichen der Beratung und Schulung. Allerdings gab es auch etliche Beschwerden, die ein Tätigwerden des TLfDI als Aufsichtsbehörde erforderten.

Auch das Jahr 2019 war beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von der seit 25. Mai 2018 neu geltenden Rechtslage geprägt. Maßgebliche Datenschutzbestimmungen finden sich nun in der Datenschutzgrundverordnung (DS-GVO) und einem geänderten Bundesdatenschutzgesetz beziehungsweise Thüringer Datenschutzgesetz. Da für die Verantwortlichen, also die Stellen, die über Zwecke und Mittel einer Datenverarbeitung entscheiden, neue Anforderungen im Hinblick auf Transparenz und Dokumentation der Datenverarbeitung gestellt wurden, bestand nach wie vor viel Beratungsbedarf. Der TLfDI führte so viele Schulungen durch, wie es seine knappen personellen Kapazitäten zuließen (siehe Beitrag Nummer 7.1). Auch Verwaltungsrichter wurden über die DS-GVO informiert. Knapp **200** Gäste folgten der Einladung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu einer Veranstaltung zum Thema Künstliche Intelligenz (KI). Im nächsten Jahr wird es eine Veranstaltung geben, in der über Profiling aufgeklärt werden soll.

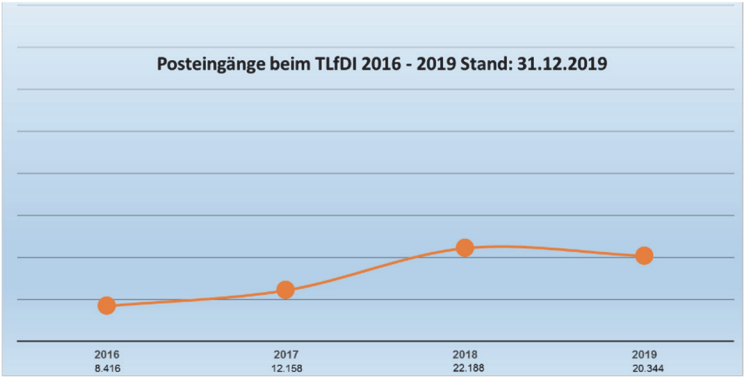
Der TLfDI beriet in einer Vielzahl von Fällen Unternehmen und Kommunen bei der Umsetzung der DS-GVO und gab Hilfestellungen bei der Lösung praktischer Probleme. Er ist der Bitte der Wirtschaftsverbände um Unterstützung gerne nachgekommen und hat sowohl bei der Industrie- und Handelskammer als auch bei der Handwerkskammer Informationsveranstaltungen zur neuen Rechtslage abgehalten.
Angesichts dieser Sachlage musste die Kontrolltätigkeit des TLfDI zunächst etwas zurückstehen. Im Verlaufe des Jahres gab es aber auch vermehrt Beschwerden, denen der TLfDI nachgegangen ist. So hat er die Durchführung der Kommunalwahl am 26. Mai 2019 begleitet und zahlreiche Beschwerden im Vorfeld der Wahl bearbeitet (siehe Beitrag Nummer 3.9). Im Bereich der Kontrolltätigkeit von Unternehmen nahm, wie bereits in den Vorjahren, die Videoüberwachung einen beträchtlichen Anteil ein.
Einen Schwerpunkt der Tätigkeit des TLfDI bildet wie immer auch der sogenannte Schulbereich, denn Thüringen hat den Vorsitz für die Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz der Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder. Der TLfDI arbeitete an der Erstellung einer FAQ-Liste des Ministeriums für Bildung, Jugend und Sport mit, die unter https://www.tlfdi.de/mam/tlfdi/datenschutz/schule/faq_datenschutz_in_schulen.pdf zu finden ist. Hierzu wird auch auf den Beitrag Nummer 3.25 verwiesen. Ein weiterer Schwerpunkt in diesem Bereich war die Beurteilung der Thüringer Schul-Cloud (siehe Beitrag Nummer 3.26) und die Einführung des Verfahrens digitale Lernumgebung für berufliche Reisende (DigLu) (siehe Beitrag Nummer 3.28). Wie schon in den vergangenen Jahren koordinierte der TLfDI auch die Zusammenarbeit zwischen dem Arbeitskreis Datenschutz-/Medienkompetenz der Aufsichtsbehörden und der Kultusministerkonferenz (KMK). Hier galt es, wichtige Intentionen zum Datenschutz in den novellierten Standards für die Lehrerausbildung zu verankern. Nach zähem Ringen ist dies gelungen. Hochschulen mit Lehrerausbildungsgängen kommen zukünftig nicht daran vorbei, angehenden Lehrerinnen und Lehrern auch Datenschutzinhalte in schulischem Kontext zu vermitteln. Ein wichtiger Schritt, der sich hoffentlich auch auf die Bereitschaft der jungen Lehrkräfte niederschlägt, ihre Schülerinnen und Schüler entsprechend zu sensibilisieren.

Im Bereich der Technik bringt die Datenschutz-Grundverordnung zahlreiche Vorschriften, was die Dokumentation der technischen Maßnahmen, die Informationspflicht des Verantwortlichen und auch die Technikfolgenabschätzung in Form der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO betrifft. Im Bezug der Informationspflicht auf Webseiten gab es sehr viele Anfragen zur Datenschutzerklärung, auf welche der TLfDI beratend reagiert hat. Ebenso wird nun stärker hinterfragt, wann die Nutzung von Cloud-Diensten zulässig ist und in welchem Rechtsrahmen dies stattfinden muss. Auch hier herrscht Unsicherheit und Aufklärungsbedürfnis. Im Bereich der Technik sind insbesondere Cloud-Anwendungen interessant, welche Daten zum Beispiel auch in die USA übermitteln könnten, da dort die globalen Player des Silicon Valley sitzen. Schwerpunkt war daher auch, diese Dienste weiter zu untersuchen. Welche Struktur besitzen sie? Sind die Daten vor externen Zugriffen ausreichend gesichert? Welches Risiko entsteht hier im Einzelnen? Diese Einzelfälle betrafen zum Beispiel die Speicherung von Schülerdaten in Storage-Diensten, Verwendung von Cloud-Systemen im Gesundheitsbereich und im öffentlichen Bereich, oder die Nutzung von Trackingverfahren eines amerikanischen Suchmaschinenanbieters innerhalb von schulischen Angeboten oder Fortbildungsplattformen. Einmal mehr wird deutlich, wie stark vernetzt hier das Internet mittlerweile agiert. Insbesondere ist nach der Datenschutz-Grundverordnung hier eine Betrachtung der Maßnahmen, gemessen an dem Risiko für Rechte und Freiheiten der Betroffenen, vorzunehmen – auch für diese Risikoabwägung war der TLfDI beratend für einige Fragestellungen tätig. Neu ist auch die Meldung von Datenpannen. Hier gab es eine große Bandbreite von Meldungen, welche von technischer und rechtlicher Seite beurteilt werden mussten und wo der TLfDI meist ergänzende Hinweise (selten auch Forderungen) zum Beheben des Sicherheitsproblems hatte.
Schließlich sucht und findet der TLfDI Kontakt zur Wirtschaft, indem er Kooperation im Vorfeld von Produktentwicklung und -anwendung anbietet. In die Vision der Smart City und der universitären oder unternehmerischen Entwicklung datenschutzrelevanter Produkte ist der TLfDI in zunehmendem Maße eingebunden und auch die Politik wird inzwischen auf diesen Ansatz des TLfDI („Kooperation statt Sanktion“) aufmerksam. Deutschland ist bei der Digitalisierung allenfalls mittelmäßig. Die Expertise in der Datenschutzaufsichtsbehörde sollte dazu genutzt werden, rechtskonforme Beschleunigungskräfte freizusetzen.

Da die „Flitterwochen“ mit der neuen Rechtslage nun nach mehr als anderthalb Jahren vorbei sind, wird sich der TLfDI künftig wieder vermehrt seiner Kontrolltätigkeit widmen. Einen ersten Aufschlag dafür stellte eine Ende des Jahres gestartete Umfrage zur Überprüfung von Webseiten Thüringer Unternehmen zum Einsatz von Analysetools dar. Die Durchführung und Ergebnisse der Umfrage wird der TLfDI im nächsten Tätigkeitsbericht ausführlich schildern.

1.2 Allgemeine Statistik und Geldbußen

Auch im ersten Kalenderjahr nach dem Wirksamwerden der Datenschutz-Grundverordnung ist die Zahl der Posteingänge beim TLfDI hoch geblieben. Meldungen von Datenpannen sowie auch der Eingang von Beschwerden haben gegenüber dem letzten Berichtsjahr zugenommen. Der TLfDI kann im Rahmen des Art. 83 Datenschutz-Grundverordnung (DS-GVO) Geldbußen in Höhe bis zu 20 Millionen Euro verhängen. Der Kriterienkatalog aus Art. 83 Abs. 2 DS-GVO ist bei jeder Entscheidung über die Verhängung einer Geldbuße und über deren Betrag in jedem Einzelfall gebührend zu berücksichtigen.



Im Jahr 2019 gab es 20.344 Posteingänge beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), die Zahl der Beschwerden betrug 667. Dabei handelt es sich um Beschwerden im Sinne des Gesetzes, die die Voraussetzungen des Art. 77 Datenschutz-Grundverordnung (DS-GVO) erfüllen, also Beschwerden von natürlichen Personen, die von der in Rede stehenden

Datenverarbeitung persönlich betroffen sind. Die Zahl der Beschwerden hat damit gegenüber dem letzten Berichtsjahr deutlich zugenommen. Insgesamt gab es 159 Meldungen nach Art. 33 DS-GVO zu Verletzungen des Schutzes personenbezogener Daten. Auch hier ist gegenüber dem letzten Berichtsjahr mit 78 Meldungen ein erheblicher Zuwachs zu verzeichnen. Es gab Fälle des Diebstahls von Rechnern, den Verlust von Akten oder sonstigen Papieren, Meldungen von Cyberangriffen, die unberechtigte Weitergabe von personenbezogenen Daten bis hin zum IT-Systemausfall.

Im Berichtszeitraum wurden zehn Verwarnungen nach Art. 58 Abs. 2 Buchstabe b) DS-GVO ausgesprochen. Diese Zahl ist dadurch gerechtfertigt, dass die Prüfverfahren im Laufe des Jahres erst angelaufen waren und viele Verfahren noch nicht abgeschlossen sind. Im nächsten Berichtsjahr ist daher mit einer wachsenden Zahl von Anordnungen zu rechnen. Zudem wurden zwei Anweisungen nach Art. 58 Abs. 2 Buchstabe c) DS-GVO auf Erteilung einer Auskunft an den Betroffenen erlassen und ein Verbot einer Datenverarbeitung nach Art. 58 Abs. 2 Buchstabe f) DS-GVO angeordnet. Weitere Maßnahmen mussten noch nicht getroffen werden, da die Verantwortlichen in den übrigen bisher durchgeführten Verfahren den Empfehlungen des TLfDI im Anhörungsverfahren nachgekommen sind.

Im Berichtszeitraum wurden beim TLfDI 16 Bußgeldverfahren nach Bundesdatenschutzgesetz alter Fassung (BDSG a. F.) bearbeitet. Diese Verfahren betreffen Verstöße, welche vor Einführung der Datenschutz-Grundverordnung begangen worden sind. Weiterhin wurden 87 Bußgeldverfahren nach der Datenschutz-Grundverordnung bearbeitet. Davon konnten 29 Bußgeldverfahren abschließend bearbeitet werden. Bußgeldverfahren enden in den meisten Fällen nach erfolgtem Einspruch mit einer Entscheidung vom Amtsgericht Erfurt, mit der Zahlung der festgesetzten Geldbuße oder mit einer Einstellung des Verfahrens. Somit verblieben zum Ende des Berichtszeitraums 74 Bußgeldverfahren beim TLfDI in Bearbeitung.

Im Berichtszeitraum wurden insgesamt 23 Bußgeldbescheide erlassen. Hiervon sind 18 Bußgeldentscheidungen rechtskräftig. Die Höhe der mit diesen Bescheiden verhangenen Geldbußen beläuft sich auf insgesamt 28.340 Euro.

Das Verhängen von Geldbußen ist in Art. 83 DS-GVO geregelt. Danach stellt der TLfDI als Aufsichtsbehörde sicher, dass die Geldbuße in jedem Einzelfall wirksam, verhältnismäßig, aber auch abschreckend ist. Wirksam und abschreckend ist eine Sanktion, wenn sie ei-

nerseits generalpräventiv geeignet ist, allgemeine Verstöße abzuwenden und andererseits aber auch spezialpräventiv geeignet ist, einen Täter von weiteren Verstößen abzuhalten (Bergt in Kühling/Buchner, DS-GVO-Kommentar, Art. 83, Rn. 50).
Bei der Entscheidung über das Verhängen einer Geldbuße und über den festzusetzenden Betrag ist der in Art. 83 Abs. 2 DS-GVO enthaltene Kriterienkatalog zu berücksichtigen. Die Geldbuße richtet sich unter anderem nach Art, Schwere und Dauer des Verstoßes. Insbesondere wird die Zahl der von der Verarbeitung betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens bewertet. Ob die Tat vorsätzlich oder fahrlässig begangen wurde, wird ebenfalls berücksichtigt. Lindernd auf den Betrag der Geldbuße wirken sich jegliche vom Verantwortlichen oder Auftragsverarbeiter getroffenen Maßnahmen aus, die zur Milderung des entstandenen Schadens für die betroffenen Personen beitragen. Zudem muss auch der Grad der Verantwortung des Verantwortlichen unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen berücksichtigt werden, wie zum Beispiel der Umfang der Zusammenarbeit mit der Aufsichtsbehörde. Erschwerend auf die Festsetzung einer Geldbuße wirken sich einschlägige frühere Verstöße des Verantwortlichen oder Auftragsverarbeiters aus. Die Höhe des Bußgeldes bemisst sich dabei auch nach der Art und Weise, wie dem TLfDI der Verstoß bekannt wurde und inwieweit frühere Anordnungen des TLfDI in selber Sache umgesetzt wurden. Zugleich müssen jegliche andere erschwerenden Umstände im Einzelfall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, in die Erwägungen zur Festsetzung eines Bußgeldes einbezogen werden.
Nach den Sanktionsvorschriften der DS-GVO ist nahezu jede Verletzung der Datenschutzbestimmungen bußgeldbewehrt. Der TLfDI kann Bußgelder zusätzlich oder anstelle der Abhilfemaßnahmen nach Art. 58 Abs. 1 DS-GVO verhängen (Art. 58 Abs. 2 Buchstabe j) DS-GVO). Soweit der Verantwortliche mehrmals gegen dieselbe Regelung verstößt, kann für jeden Verstoß ein Bußgeld festgesetzt werden. Je nach Zeitabfolge der Verstöße werden diese in einem Bußgeldbescheid geahndet. Soweit ein Datenschutzverstoß nach Zahlung eines Bußgeldes nicht abgestellt worden ist, kann wegen desselben Verstoßes erneut ein Bußgeldbescheid erlassen werden.

Die Schwerpunkte der Bußgeldverfahren beim TLfDI im Jahr 2019 konzentrierten sich auf

- Videoüberwachungsanlagen,
- private Abrufe aus polizeilichen Informationssystemen durch Polizeibeamte,
- nicht erteilte Auskünfte gegenüber dem TLfDI nach Art. 58 Abs. 1 DS-GVO,
- nicht erteilte Auskünfte gegenüber den Betroffenen nach Art. 15 Abs. 1 DS-GVO,
- fehlende Meldung einer Datenpanne nach Art. 33 DS-GVO,
- fehlende Information nach Art. 13 DS-GVO,
- unbefugte Verarbeitung personenbezogener Daten aus einem Mandantenverhältnis durch Rechtsanwälte,
- GPS-Überwachung von Arbeitnehmern,
- Übermittlung von Mieter- und Eigentümerdaten im Immobiliengewerbe,
- Übermittlung von E-Mail-Adressen,
- private Nutzung von Kundendaten durch Versicherungsmakler.

2. Themengebiete

© Spencer- 3D Man Office - fotolia.com

2.1 „Es ist des Lernens kein Ende“ – Irrtümer über die DS-GVO

Der „alte Behördengrundsatz: Das haben wir schon immer so gemacht“ war auch bei Einführung der Datenschutz-Grundverordnung (DS-GVO) absolut hinderlich und dringend „in die Mottenkiste“ zu legen: Natürlich muss sich einerseits jeder Rechtsanwender einer öffentlichen Stelle darüber informieren, was sich für Neuerungen aus dem nicht gerade einfach und verständlich gestalteten Datenschutzrecht auf europäischer und nationaler Ebene ergeben. Andererseits können die Bürgerinnen und Bürger aber nicht annehmen, dass mit Hilfe der DS-GVO nun jegliche Datenverarbeitung untersagt ist. Für jedermann gilt: Informieren Sie sich über die DS-GVO – gern beim TLfDI.

Das Zitat aus der Überschrift stammt vom Komponisten und Musiker Robert Schumann. Das Gleiche hätte dieser auch gut und gern über die Europäische Datenschutz-Grundverordnung (DS-GVO) und ihre Anwendung sagen können. Denn auch im Berichtsjahr häuften sich Schreiben und Beschwerden beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), deren Verfasser die DS-GVO gründlich missverstanden hatten. Dies ist angesichts der Komplexität dieses Regelwerks und seiner vielen unbestimmten

Rechtsbegriffe nicht verwunderlich, und niemand wurde und wird vom TLfDI wegen einer Frage rund um die DS-GVO abgewiesen. Damit das Robert-Schumann-Zitat auch in diesem Tätigkeitsbericht mit Leben erfüllt wird, werden hier beispielhaft drei Irrtümer zur DS-GVO aus dem letzten Jahr genannt, die dem TLfDI zur Kenntnis gelangt sind:

Nicht wenige Beschwerdeführer, die sich an den TLfDI wandten, waren der Rechtsauffassung, dass die DS-GVO nunmehr jegliche Datenverarbeitung verbiete und daher auch ihre personenbezogenen Daten nicht von einer genannten Behörde verarbeitet werden dürften. In vielen dieser Fälle musste der TLfDI jedoch Folgendes mitteilen: Gemäß Artikel 8 Absatz 2 der Charta der Grundrechte der Europäischen Union (GR-Charta) dürfen personenbezogene Daten unter anderem nur dann verarbeitet werden, wenn es dafür eine gesetzlich geregelte legitime Grundlage gibt. Dies ist das **Verbotsprinzip mit Erlaubnisvorbehalt**, das auch in Art. 6 Abs. 1 Satz 1, und hier insbesondere Buchstabe c) DS-GVO umgesetzt ist. Somit war in jedem Einzelfall eines Beschwerdeführers zu prüfen, ob es eine besondere Rechtsgrundlage gab, die der Behörde die Verarbeitung der personenbezogenen Daten des Beschwerdeführers gestattete.

Ein weiterer Irrtum, dem auch nicht ganz unerfahrene Freunde des Datenschutzes zuweilen aufsaßen, war der, dass bestimmte Regelungen der DS-GVO pauschal nur für den nicht-öffentlichen Bereich, nicht aber für den öffentlichen Bereich gelten würden, weil sie auf den öffentlichen Bereich gar nicht anwendbar seien. Auf diese Problematik antwortete der TLfDI wie folgt:

Grundsätzlich sind alle Regelungen der DS-GVO sowohl auf öffentliche Stellen (Landesbehörden und Kommunalbehörden) als auch auf nicht-öffentliche Stellen (zum Beispiel Unternehmen) anwendbar, es sei denn, die DS-GVO schließt für ihren Anwendungsbereich eine der beiden genannten Stellen ausdrücklich aus. Letzteres ist zum Beispiel in Art. 6 Abs. 1 Satz 2 DS-GVO der Fall. Danach gilt die Bedingung der Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO (= Verarbeitung ist zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich) nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Ein häufig auftretender Irrtum der Behörden, die hier fälschlicherweise eine Rechtsgrundlage für ihre Datenverarbeitung erkannt haben wollten. Somit weist die DS-GVO selbst und klar darauf

hin, welche ihrer Regelungen für Behörden als öffentliche Stellen nicht anzuwenden sind.
Schwieriger wird es, wenn ein EU-Mitgliedstaat sich der in der DS-GVO enthaltenen Öffnungsklauseln bedient, die bewirken, dass im nationalen Datenschutzrecht von den Vorgaben der DS-GVO abgewichen werden kann. In solchen Fällen muss der Rechtsanwender neben der DS-GVO immer auch die Landesnormen, in Thüringen also meistens das Thüringer Datenschutzgesetz (ThürDSG) zu Rate ziehen. Ein Beispiel dafür: Gemäß Art. 23 Abs. 1 Satz 1 DS-GVO kann das Auskunftsrecht der betroffenen Person nach Art. 15 Abs. 1 DS-GVO auch durch Rechtsvorschriften der Mitgliedstaaten eingeschränkt werden, wenn dies zum Beispiel zur Wahrung der nationalen Sicherheit (Art. 15 Abs. 1 Satz 1 Buchstabe a) DS-GVO) oder zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen (Art. 15 Abs. 1 Satz 1 Buchstabe i) DS-GVO) erforderlich ist. Von dieser Einschränkungsmöglichkeit hat der Thüringer Gesetzgeber in § 21 ThürDSG Gebrauch gemacht und dort für öffentliche Stellen geregelt, dass diese das Auskunftsrecht nach Art. 15 DS-GVO beschränken können, wenn zum Beispiel gemäß § 21 Abs. 1 Nr. 1 ThürDSG die Auskunftserteilung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, oder wenn gemäß § 21 Abs. 1 Nr. 2 ThürDSG die personenbezogenen Daten oder die Tatsache ihrer Speicherung wegen einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der Rechte und Freiheiten einer anderen Person, geheim gehalten werden müssen. Anhand dieses Beispiels wird deutlich, dass die Anwender des Datenschutzrechts nicht mehr wie bisher, sich nur ein Gesetz „auf den Tisch legen“ dürfen, sondern neben der DS-GVO immer noch das ThürDSG (für öffentliche Stellen) oder das Bundesdatenschutzgesetz (für nichtöffentliche Stellen) zu Rate ziehen müssen.
Offensichtlich gar kein Gesetz richtig gelesen hatte ein Landratsamt, das dem folgenden schweren Irrtum unterlag: Das Amt für Kommunalaufsicht des Landratsamtes, das als Widerspruchsbehörde für das Straßenausbaubeitragsrecht zuständig sei, hatte allen Widerspruchsführern eine Einwilligungserklärung für die Datenverarbeitung im Rahmen der Widerspruchsbearbeitung übersandt und sie ferner darüber belehrt, dass ihr Widerspruch gegen den angegriffenen Bescheid ohne Sachprüfung als unzulässig zurückgewiesen werde, wenn die Einwilligungserklärung in die Datenverarbeitung zum Zweck der Be-

arbeitung des Widerspruchsverfahrens nicht unterschrieben zurückgesandt werde. Die sachlich nicht zu haltende Rechtsauffassung hatte bis dato auch der TLfDI noch nicht kennengelernt: Er wies die Kommunalaufsichtsbehörde unverzüglich telefonisch und schriftlich auf Folgendes hin: Eine Einwilligungserklärung sei zur Widerspruchsbearbeitung im geschilderten Fall mitnichten erforderlich. Denn für die Durchführung und Bearbeitung von Widersprüchen gelten auch nach Einführung der DS-GVO die §§ 68 ff. der Verwaltungsgerichtsordnung beziehungsweise das weitere Fachrecht, hier konkret § 15 Thüringer Kommunalabgabengesetz und § 357 Abgabenordnung sowie die dazugehörigen Zuständigkeitsregelungen (zum Beispiel § 118 Thüringer Kommunalordnung) weiter. Daher erfolgte und erfolgt die Bearbeitung von Widersprüchen auch in den Angelegenheiten des Straßenausbaubeitragsrechts verpflichtend auf der Grundlage eines Gesetzes. Demzufolge war und ist im geschilderten Sachverhalt das Amt für Kommunalaufsicht berechtigt, die personenbezogenen Daten der Widerspruchsführer auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe c) und Buchstabe e) DS-GVO zu erheben. Art. 6 Abs. 1 Satz 1 Buchstabe c) und Buchstabe e) regeln dabei Folgendes: *„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist (...)*
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt,
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde [...].
Zudem bestimmt Art. 6 Abs. 3 Satz 1 DS-GVO Folgendes: *„Die Rechtsgrundlage für die Verarbeitungen gemäß Abs. 1 Buchstaben c) und e) wird festgelegt durch a) Unionsrecht oder b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.“* Er enthält mithin eine Öffnungsklausel für das nationale (Prozess-)Recht.
Weiterhin wies der TLfDI das Amt für Kommunalaufsicht darauf hin, dass eine Einwilligung – auf die das Amt seine Verarbeitung personenbezogener Daten stützen wollte – gemäß Art. 4 Nr. 11 DS-GVO freiwillig erteilt werden müsse. Dieses Freiwilligkeitskriterium ist gerade dann nicht gegeben, wenn die Einwilligung an eine Bedingung geknüpft wird, nämlich hier: Widerspruchsbearbeitung nur gegen Erteilung der Einwilligung.
Abschließend bat der TLfDI das Amt für Kommunalaufsicht dringend darum zu prüfen, ob bereits von ihm Widersprüche aufgrund fehlen-

der vorliegender Einwilligung als unzulässig zurückgewiesen worden seien. Dies wäre, so der TLfDI, in jedem Fall rechtsfehlerhaft.

2.2 Die Hambacher Erklärung: ein erstes Rahmenwerk zur Regulierung von künstlicher Intelligenz

Die Datenschutzaufsichtsbehörden haben sich in der „Hambacher Erklärung“ erstmals grundlegend zum Thema Künstliche Intelligenz – KI – positioniert. Die gestellten Forderungen sind umfangreich und der Komplexität des Themas geschuldet. Inwieweit diese in der Praxis umgesetzt werden können und welche Probleme dabei auftreten werden, muss sich zukünftig zeigen.

Das Thema „Künstliche Intelligenz“ wird von den Datenschutzaufsichtsbehörden des Bundes und der Länder schon seit Jahren beobachtet. Sehr viele Alltagsprodukte wie smarte Lautsprecher beziehungsweise Assistenten, Textkorrektur-Mechanismen, Bilderkennungs- und Verbesserungsalgorithmen in Smartphone-Kameras, aber auch so gewöhnliche Dinge wie die Schaltung von Werbung auf Webseiten, Vorschläge für News bei Facebook, Bing oder Yahoo, die Reihenfolge von Suchergebnissen bei Suchmaschinen im Internet, Fahrassistenzsysteme, Online-Fitness-Coaches und so weiter enthalten Komponenten, welche mit „Künstlicher Intelligenz“ arbeiten.
Künstliche Intelligenz suggeriert hierbei ein System, welches Aufgaben lösen kann, für die im Normalfall „menschliche Intelligenz“ benötigt werden würde. In Wirklichkeit sind solche Systeme nicht intelligent, da sie ihre Umgebung und ihre Aufgaben nicht wirklich verstehen. Vielmehr können solche Systeme wiederkehrende (und teilweise komplexe) Muster erkennen und abstrakt zu den Ergebnissen weiterverarbeiten, welche sich die Anbieter wünschen. Hierunter fallen zum Beispiel Spracherkennung, Erkennung von Gesichtern, häufig genutzte Textpassagen, aber auch das Erkennen von persönlichen Eigenschaften wie Alter, Geschlecht oder eigene Interessen.
Die Algorithmen der „Künstlichen Intelligenz“ können dabei nur die für ein Ergebnis typischen „Ausgangsdatenmuster“ lernen (zum Beispiel typische Merkmale in den aufgenommenen Sprachsignalen eines Mikrofons für das Wort „Text“). Der Algorithmus kennt dabei weder die Bedeutung des Ergebnisses noch die Bedeutung der Eingangssignale; er lernt nur, bei den typischen Eingangssignalen das trainierte Ergebnis auszugeben.

Aus datenschutzrechtlicher Sicht hat diese Eigenschaft gleich mehrere Herausforderungen zur Folge: Einmal sind für dieses Training sehr große Datenmengen notwendig, um gute und robuste Ergebnisse zu liefern (das Wort „Text“ kann zum Beispiel schnell oder langsam, hoch oder tief, laut oder leise, sächsisch, hessisch oder schwäbisch ausgesprochen werden) – daher sind Algorithmen der Künstlichen Intelligenz durch ihre Funktionsweise grundsätzlich datenhungrig. Außerdem kann der Zweck vom Anbieter frei bestimmt werden. Da das System den Daten keine „Bedeutung“ zuordnen kann, können aus den gleichen Eingangsdaten (zum Beispiel das Sprachsignal für das Wort „Text“) ganz unterschiedliche Ergebnisse abgeleitet werden (zum Beispiel „Wurde ‚Text‘ erkannt?“, aber auch „Alter oder Geschlecht des Sprechers“ sind möglich, eventuell sogar, welche Person gesprochen hat). Das Training wählt dann aus dem Ausgangssignal nur jeweils andere – für das Problem relevante – Informationen des Ursprungssignals aus, um ein gewünschtes Ergebnis zu liefern.
Dieses Werkzeug der Signalerkennung kann für den Datenschutz unkritisch sein, wenn keine personenbezogenen Daten verarbeitet werden, es kann aber auch hochgradig kritisch sein (zum Beispiel bei Schätzung von Interessen, persönlichen Merkmalen, eventuell Krankheiten, politischen Meinungen und so weiter). Für die Fälle, in denen einmal Daten mit Personenbezug zum Training für Algorithmen der „Künstlichen Intelligenz“ genutzt werden, aber auch für den Fall, dass der Algorithmus selber Ergebnisse mit Personenbezug produziert, hat die „98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder“ im April 2019 eine Entschließung verabschiedet, welche die Grenzen der zulässigen Nutzung von KI-Systemen aufzeigen soll, und sieben datenschutzrechtliche Anforderungen formuliert – die „Hambacher Erklärung“. Diese ist unter https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/190403_final_hambacher erklarung_aktualisiert.pdf zu finden.

Die Hambacher Erklärung stellt dabei grundlegende Forderungen auf:

1. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 Datenschutz-Grundverordnung (DS-GVO) nicht allein der Maschine überlassen werden.

2. Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchstabe b) DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt.
3. KI-Systeme müssen transparent, nachvollziehbar und erklärbar sein. Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 Buchstabe a) DS-GVO). Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).
4. KI muss Diskriminierung vermeiden. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar.
5. Für KI gilt der Grundsatz der Datenminimierung. Ihre Systeme nutzen typischerweise große Bestände von Trainingsdaten. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Die Verarbeitung personenbezogener Daten muss stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.
6. KI braucht Verantwortlichkeit: Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff. DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.
7. KI benötigt technische und organisatorische Standards: Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisato-

rische Maßnahmen gemäß Art. 24 und 25 DS-GVO zu treffen, wie zum Beispiel Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln, ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

Auch die Datenethikkommission der Bundesregierung hat sich eingehender mit dem Thema befasst (Empfehlungen siehe hier https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/datenethikkommission/empfehlungen-datenethikkommission.pdf?__blob=publicationFile&v=2) und ist zu dem Ergebnis gekommen, dass nicht nur die wirtschaftlichen Interessen der technischen Möglichkeiten von KI in der Strategie der Bundesregierung berücksichtigt werden dürfen, sondern durchaus auch die gesellschaftlichen Grundwerte beachtet werden müssen. Auch dazu tragen die Forderungen der Hambacher Erklärung bei.

Auf der Grundlage der Hambacher Erklärung vom 3. April 2019 hat die 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem zusätzlichen Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Auch hier hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit mitgewirkt. Dieses Positionspapier wurde zusammen mit einer entsprechenden Entschließung im November 2019 veröffentlicht (siehe https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/entschliessung_top_06_im_dsk-format_clean_dsk.pdf).

Die in der Hambacher Erklärung festgelegten

rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, welche auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind. So ist zum Beispiel für den ersten Verarbeitungsschritt (Generierung und Veredelung von Trainingsdaten) darauf zu achten, dass der Trainingsdatensatz datenminimal wird, das heißt, wenn möglich synthetische Daten genutzt werden, aber auch nur so viele Daten wie nötig, um den gewünschten Funktionsumfang zu ermöglichen sowie über Dimensionsreduktion oder andere Mechanismen eine Anonymisierung oder Pseudonymisierung herzustellen. Weiterhin muss auch transparent gemacht werden, welche Art der Daten zum Training genutzt werden, wie sichergestellt wird, dass die Daten das Problemfeld hinreichend repräsentieren (ohne eine Diskriminierung zu verursachen) und inwieweit weitere Daten (und eventuell auch Nutzerdaten) zum Nachtraining des Systems genutzt werden. Für die Trainingsphase wäre zum Beispiel dafür zu sorgen, dass die Güte des Systems im Sinne der Fehleranfälligkeit für den Nutzer beschrieben wird, sodass erkennbar wird, welche personenbezogenen Ergebnisse das System aus den Eingangsdaten erzeugt und welche Möglichkeiten der Nutzer zur Intervention im Fehlerfall besitzt. Eine vollständige Erklärbarkeit der Datenverarbeitung ist hingegen nicht in jedem Fall sinnvoll oder durchführbar. Das Positionspapier ist unter folgendem Link verfügbar: https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/positionspapier_kunstliche_intelligenz.pdf.

Insgesamt steht die Diskussion zum Datenschutz in Verbindung mit KI-Systemen noch am Anfang. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

2.3 Die Datenschutzordnung für parlamentarische Aufgaben des Landtags und seiner Fraktionen und ihre Kontrolle – ohne den TLfDI

Datenschutzkontrolle ohne den TLfDI: § 2 Abs. 6 Satz 3 und 4 Thüringer Datenschutzgesetz in Verbindung mit § 1 Abs. 1 und § 17 Abs. 1 der Parlamentarischen Datenschutzordnung (ParlDSO) regelt, dass der Ältestenrat des Thüringer Landtags die Einhaltung der Bestimmung der ParlDSO sowie der besonderen Vorschriften überwacht. Das bedeutet: Sofern ein Betroffener einen Datenschutzverstoß im Rahmen der Wahrnehmung parlamentarischer Aufgaben durch den Landtag, seiner Organe, Gremien oder seiner mit einem freien Mandat ausgestatteten Mitgliedern geltend machen will, muss er sich an den Ältestenrat des Landtags wenden. Soweit Landtagsfraktionen einen mutmaßlichen Datenschutzverstoß im Rahmen der Wahrnehmung ihrer parlamentarischen Angelegenheiten begehen, muss der Betroffene sich direkt bei der jeweiligen Fraktion beschweren.

Eine interessante Frage, die immer wieder in Schreiben und Beschwerden an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) während des Berichtszeitraums gestellt wurde, war jene, ob er auch für die datenschutzrechtliche Kontrolle der Fraktionen des Thüringer Landtags, seiner Abgeordneten sowie Mitarbeiter und Wahlkreismitarbeiter der Abgeordneten im Rahmen ihrer parlamentarischen Tätigkeit zuständig sei.
Der TLfDI konnte diese Frage stets mit einem klaren Nein beantworten, und zwar aus folgenden Gründen:

- In Art. 2 Abs. 2 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) heißt es wörtlich: „Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht dem Anwendungsbereich des Unionsrechts unterfällt."
- Die Parlamentarische Tätigkeit des Bundestags und der Landtage wird unter Hinweis auf Art. 4 Abs. 1 des Vertrages über die EU (EUV) nicht vom Anwendungsbereich des Unionsrechts erfasst. Art. 4 Abs. 1 EUV hat folgenden Wortlaut: „Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben gemäß Art. 5 EUV bei den Mitgliedstaaten."
- Treffend zusammengefasst ist die Nicht-Anwendbarkeit der DS-GVO für den parlamentarischen Bereich in der Begründung des

Gesetzentwurfs der Bayerischen Staatsregierung für ein neues Bayerisches Datenschutzgesetz (BayDSG). Hier (Drucksache 17/19628, Seite 31 der Begründung zu Art. 1 BayDSG) heißt es: „Die parlamentarische Tätigkeit des Landtags unterliegt als Kernbereich des innerstaatlichen Organisationsrechts nicht dem Anwendungsbereich der DS-GVO, sodass landesrechtliche Regelungen zu deren Durchführung nicht zwingend sind."

- Auch der Thüringer Landtag hat sich im Rahmen der Anpassung des Thüringer Datenschutzgesetzes (ThürDSG) an die DS-GVO und die JI-Richtlinie dafür entschieden, dass die parlamentarische Tätigkeit des Landtags nicht der DS-GVO unterfallen soll. Deshalb regelt § 2 Abs. 6 Satz 3 und Satz 4 ThürDSG Folgendes: „Die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag sowie der parlamentarischen Tätigkeit der Abgeordneten einschließlich der Fraktionen unterliegt nicht den Bestimmungen dieses Gesetzes. Der Landtag erlässt insoweit eine seiner verfassungsrechtlichen Stellung entsprechende Datenschutzordnung."
- Den § 2 Abs. 6 Satz 4 ThürDSG „mit Leben erfüllt" hat der Thüringer Landtag am 16. Oktober 2019, als er eine parlamentarische Datenschutzordnung (ParlDSO) verabschiedete. Leider enthält dieses Regelwerk keine exakte Definition des Begriffs der parlamentarischen Aufgaben. Stattdessen regelt § 1 Abs. 2 ParlDSO, dass ihre Normen keine Anwendung finden, wenn personenbezogene Daten zum Zweck der **Wahrnehmung von Verwaltungsaufgaben** verarbeitet werden. Dann also findet die DS-GVO Anwendung und der TLfDI ist zuständig. Verwaltungsaufgaben sind gemäß § 1 Abs. 2 Satz 2 ParlDSO insbesondere
  1. wirtschaftliche Angelegenheiten des Landtags,
  2. die Personalverwaltung des Landtags,
  3. die Ausübung des Hausrechts und der Polizeigewalt im Sinne des Art. 57 Abs. 3 Satz 2 der Verfassung des Freistaats Thüringen und
  4. die Ausführung der Gesetze, soweit diese der Präsidentin beziehungsweise dem Präsidenten des Landtags zugewiesen sind und nicht in unmittelbarem Zusammenhang mit der Wahrnehmung parlamentarischer Aufgaben stehen.

Somit wird die weitere Anwendung der ParlDSO auf der einen, und die Arbeit mit dem ThürDSG auf der anderen Seite zeigen, ob diese beiden Regelwerke die Sicherstellung eines umfassenden Datenschut-

zes reibungslos und stets voneinander abgrenzbar gewährleisten. Dabei helfen soll mutmaßlich die in § 1 Abs. 4 ParlDSO enthaltene Auslegungsregel, wonach ein einheitlicher Lebenssachverhalt der ParlDSO unterliegt, soweit er im Schwerpunkt der Wahrnehmung parlamentarischer Aufgaben zuzurechnen ist.
Weiterhin ist noch auf Folgendes hinzuweisen:
Erstens: Die ParlDSO erinnert in ihrem Aufbau an die DS-GVO, denn sie enthält in § 2 zunächst die Begriffsbestimmungen, regelt in § 3 die Voraussetzungen der Zulässigkeit einer Datenverarbeitung, geht in § 4 auf die Einwilligung in eine Datenverarbeitung ein, benennt in § 7 die Informations-, Dokumentations- und die Beteiligungsplattformen und zählt ab § 8 die Betroffenenrechte auf. Deshalb kann der Einwand hier nicht ganz von der Hand gewiesen werden, warum die Abgeordneten des Thüringer Landtags es sich nicht einfacher gemacht und kraft ihrer Unabhängigkeit entschieden haben, dass auch für den parlamentarischen Bereich die DS-GVO zur Anwendung gelangt – selbstverständlich ohne Aufsichtsbefugnisse des TLfDI.
Zweitens: Beachtenswert ist in der ParlDSO ihr § 17, der die Datenschutzkontrolle regelt. Zuständig für die Überwachung der Einhaltung der ParlDSO sowie der besonderen Rechtsvorschriften ist danach der Ältestenrat des Landtags. Ausgenommen von dieser Kontrolle ist gemäß § 17 Abs. 1 Satz 2 ParlDSO die Verarbeitung personenbezogener Daten durch die Parlamentarische Kontrollkommission und die G10-Kommission sowie weiterer Gremien, soweit durch Gesetz eine abweichende Datenschutzkontrolle bestimmt ist. Die Aufgaben des Ältestenrats werden in § 17 Abs. 2 und Abs. 3 näher bestimmt:
Gemäß § 17 Abs. 2 ParlDSO nimmt der Ältestenrat Beschwerden und Beanstandungen betroffener Personen oder von Verantwortlichen entgegen und geht Vorgängen nach, die Anlass zu einer Überprüfung geben. Den Verantwortlichen kann der Ältestenrat gemäß § 17 Abs. 3 Satz 3 ParlDSO Empfehlungen zur Verbesserung des Schutzes personenbezogener Daten zum Zweck der Wahrnehmung parlamentarischer Aufgaben geben. Da hier wie auch an keiner anderen Stelle der ParlDSO eine Regelung über Sanktionen oder gar Geldbußen für den Ältestenrat enthalten ist, sind ihm keine Abhilfebefugnisse eingeräumt.
Abschließend ist auf § 17 Abs. 4 Satz 1 ParlDSO hinzuweisen, wonach die Fraktionen im Landtag die von ihnen selbst durchgeführte Datenverarbeitung in eigener Verantwortung überwachen. Ferner regelt § 17 Abs. 4 Satz 3 ParlDSO, dass die Fraktionen im Einzelfall

oder für bestimmte Angelegenheiten des Datenschutzes die Kontrolle auf den Ältestenrat übertragen können. Das bedeutet im Umkehrschluss, dass sowohl die Abgeordneten als Funktionsträger als auch die Mitarbeiter einer Landtagsfraktion in ihrer parlamentarischen Tätigkeit nicht der Kontrolle des TLfDI unterliegen.

2.4 Der TLfDI vor Ort

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm im Berichtszeitraum im öffentlichen Bereich wieder vermehrt Vor-Ort-Kontrollen vor. Diese erfolgten bei unterschiedlichen öffentlichen Stellen.

In diesem Jahr nahm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wieder vermehrt seine Kontrolltätigkeit vor Ort bei den verantwortlichen öffentlichen Stellen auf.
Zur Wahrnehmung seiner Aufgaben stehen dem TLfDI die Befugnisse nach Art. 58 der Datenschutz-Grundverordnung (DS-GVO) zur Verfügung. So kann der TLfDI gemäß Art. 58 Abs. 1 DS-GVO im Rahmen seiner Untersuchungsbefugnisse unter anderem vom Verantwortlichen verlangen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben erforderlich sind. Der TLfDI muss gemäß § 7 Abs. 1 Satz 2 des Thüringer Datenschutzgesetzes (ThürDSG) vor Ausübung der Abhilfebefugnisse gemäß Art. 58 Abs. 2 DS-GVO (zum Beispiel Verwarnungen, Anweisungen, Verbote verhängen) eine Stellungnahme der verantwortlichen Stelle unter Einbeziehung der jeweils obersten Landesbehörde und Aufsichtsbehörde anfordern. § 7 Abs. 1 Satz 2 ThürDSG lautet: „Kommt der Landesbeauftragte für den Datenschutz zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt er dies dem Verantwortlichen vor Ausübung seiner Befugnisse nach Art. 58 Abs. 2 der DS-GVO mit und fordert diesen binnen angemessener Frist zur Stellungnahme auf. Die zuständige oberste Landesbehörde und die Aufsichtsbehörde sind davon zu unterrichten.“
Dem TLfDI bleibt es gegenüber öffentlichen Stellen verwehrt, die sofortige Vollziehung seiner Maßnahmen anzuordnen. § 9 Abs. 1 Satz 2 ThürDSG verweist insoweit auf § 20 Abs. 7 des Bundesdatenschutzgesetzes. Dieser normiert, dass die Aufsichtsbehörde gegenüber einer

Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Abs. 2 Satz 1 Nr. 4 der Verwaltungsgerichtsordnung anordnen darf. Das bedeutet im Ergebnis, dass der TLfDI abwarten muss, bis die aufschiebende Wirkung entfällt. Das geschieht in folgenden Fällen: Entweder hat gegen den Verwaltungsakt innerhalb eines Monats nach dessen Zustellung niemand einen Rechtsbehelf eingelegt oder, sollte Klage erhoben worden sein, die abschließende gerichtliche Entscheidung ist rechtskräftig geworden. Wie lange ein Gerichtsverfahren dauern kann, hängt immer vom Einzelfall ab.
Im Rahmen von Datenverarbeitungen, die unter die JI-Richtlinie fallen (also vor allem Datenverarbeitungen aus dem Polizeibereich), steht dem TLfDI ein Beanstandungsrecht gemäß § 7 Abs. 6 ThürDSG zu, wenn der TLfDI Verstöße gegen die Vorschriften des Datenschutzes feststellt.
Der TLfDI möchte an dieser Stelle jedoch festhalten, dass die öffentlichen Stellen in den meisten Fällen gut mit dem TLfDI zusammenarbeiten und Maßnahmen und Forderungen des TLfDI umsetzen.
Die Kontrolltätigkeit des TLfDI vor Ort erstreckte sich in diesem Berichtsjahr auf verschiedene datenschutzrechtlich relevante Bereiche. So erfolgte beispielsweise eine Kontrolle bei einem Thüringer Rettungsdienstverband, um den Umgang mit personenbezogenen Daten im Hinblick auf die Nutzung des Gleichwellenfunkkanals zu prüfen. Hintergrund war ein zuvor erfolgter Hackerangriff, bei dem möglicherweise personenbezogene Daten an unberechtigte Dritte gelangten. Die Prüfung, ob tatsächlich personenbezogene Daten „abgefangen“ wurden, bedurfte jedoch noch einer weiteren Prüfung unter Zuhilfenahme der zuständigen Polizeidienststelle. Über das Ergebnis der Ermittlungen wird der TLfDI im nächsten Tätigkeitsbericht informieren.
Darüber hinaus kontrollierte der TLfDI beim Amt für Verfassungsschutz und beim Thüringer Landeskriminalamt (TLKA) die Anti-Terror-Datei. Das Antiterrordateigesetz (ATDG) sieht gemäß § 10 Abs. 1 ATDG vor, dass die Kontrolle der Durchführung des Datenschutzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit obliegt. Die datenschutzrechtliche Kontrolle der Eingabe und der Abfrage von Daten durch eine Landesbehörde richtet sich nach dem Datenschutzgesetz des Landes. Datenschutzrechtliche Verstöße konnten dabei nicht festgestellt werden. Lediglich die technische Umsetzung der Speicher- und Löschfristen werden durch das TLKA nochmal einer Prüfung unterzogen, um sicherzustellen, dass lediglich ATD-relevante Personen in der Datei gespeichert sind.

Auch der Einsatz einer Videoüberwachungsanlage einer öffentlichen Stelle gelangte in den Fokus des TLfDI. Hintergrund hierfür war die Anfrage eines Bürgers, der sich über die doch zahlreichen Videokameras wunderte, die die öffentliche Stelle an dem Gebäude anbringen ließ. Im Zuge der Vor-Ort Kontrolle stellte sich unter anderem heraus, dass die erstellten Unterlagen teilweise veraltet waren und sich auf alte Rechtsgrundlagen bezogen. Die angegebenen Rechtsgrundlagen entsprachen zudem nicht der Norm, die für diese Videoüberwachung in Betracht kam. In diesem Fall war es § 30 ThürDSG. Diese Prüfung konnte im Berichtszeitraum noch nicht beendet werden, sodass hierüber im nächsten Tätigkeitsbericht informiert wird.
Einer anonymen Eingabe über mögliche Verletzungen des Datenschutzes ging der TLfDI auch in einer anderen Thüringer Kommune nach. In der anonymen Beschwerde wurden der Mangel an ausreichenden Schutzmaßnahmen bezüglich des IT-Systems sowie unzureichende technische organisatorische Maßnahmen beanstandet, die dazu geführt hätten, dass möglicherweise Mitarbeiter die Konten von anderen Mitarbeitern einsehen konnten. Im Zuge der Kontrolle musste der TLfDI vor Ort einige datenschutzrechtliche Mängel feststellen. Ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) existierte beispielsweise nicht. Schlimmer wog jedoch die Tatsache, dass sich das IT-System im Toilettenraum befand. Umringt von einer separaten, aber von oben und unten offenen Kabinenumfassung stand dort das IT-System dieser öffentlichen Stelle. Damit war den technischen und organisatorischen Anforderungen mitnichten Rechnung getragen. Dass Mitarbeiter die Konten von anderen Mitarbeitern einsehen konnten, bestätigte sich indes nicht. Auch über diese Prüfung wird im nächsten Tätigkeitsbericht informiert, da der Vorgang im Berichtszeitraum nicht abgeschlossen werden konnte.
Es bleibt also spannend!

2.5 Recht auf Kopie im Rahmen der Auskunftserteilung?

Der Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) ist ein zentrales Betroffenenrecht. Das „Recht auf Kopie“ (Art. 15 Abs. 3 DS-GVO) ist nicht wörtlich zu verstehen, sondern im Sinne des DS-GVO auszulegen.

Die Datenschutz-Grundverordnung (DS-GVO) steht ganz im Lichte der Transparenz der Datenverarbeitung für die betroffenen Personen.

Dabei ist das Auskunftsrecht, dass sich in Art. 15 DS-GVO befindet, ein zentrales Betroffenenrecht. Die Bestimmung regelt, dass jede betroffene Person zunächst das Recht hat, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten vom Verantwortlichen verarbeitet werden. Wenn dies der Fall ist, hat der Verantwortliche grundsätzlich über folgende Informationen Auskunft zu geben:

- die Verarbeitungszwecke,
- die Kategorien der personenbezogenen Daten,
- die Empfänger oder die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
- die geplante Speicherdauer beziehungsweise die Kriterien für die Festlegung dieser Dauer,
- das Bestehen des Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung sowie das Widerspruchsrecht gegen die Verarbeitung,
- das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde,
- bei Dritterhebung alle Informationen über die Herkunft der Daten,
- bei Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling aussagekräftige Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Wegen des technikneutralen Ansatzes der DS-GVO erstreckt sich der Auskunftsanspruch auf jede Art der Verarbeitung von personenbezogenen Daten, das heißt auf die automatisierte ebenso wie auf die nicht automatisierte Verarbeitung. Die betroffene Person hat grundsätzlich ein Wahlrecht, ob sie nur die Auskunft darüber verlangt, ob der Verantwortliche sie betreffende personenbezogene Daten verarbeitet. Sofern dies der Fall ist, kann sie stets von ihrem Recht Gebrauch machen, Auskünfte zu den oben aufgeführten Informationen zu erhalten. Kern des Auskunftsrechts ist dabei der Anspruch auf Auskunft über die konkret zu einer Person verarbeiteten Daten. Diese Auskunft muss, den Voraussetzungen des Art. 12 DS-GVO folgend, in einfacher und verständlicher Sprache gegeben werden. Außerdem ist die Auskunft vollständig zu erteilen.

Zudem ist in Art. 15 Abs. 3 geregelt, dass der Verantwortliche eine „Kopie“ der personenbezogenen Daten, die Gegenstand der Verarbei-

tung sind, zur Verfügung stellt. Über die Reichweite dies „Rechts auf Kopie“ besteht Unklarheit. Fraglich ist, ob es sich um einen eigenen Rechtsanspruch des Betroffenen handelt oder lediglich um eine Form der Ausgestaltung des Auskunftsrechts nach Art. 15 Abs. 1 DS-GVO. Fest steht aber, dass der Verantwortliche eine „Kopie“ zu erstellen hat, wenn der Betroffene dies verlangt. Hier ist zu beachten, dass der Begriff „Kopie“ im Deutschen anders verwandt wird als im Englischen der Begriff „copy“. Nach dem englischen Wortlaut der DS-GVO ist eine „copy“ zu erstellen, was so viel bedeutet wie eine Abschrift und nicht eine Ablichtung wie im Deutschen.
Eine klare Vorgabe, was genau der Verantwortliche der betroffenen Person zur Verfügung zu stellen hat, ist in der DS-GVO nicht enthalten. Eine Kopie ist jedenfalls nach dem Wortlaut des Art. 15 Abs. 3 DS-GVO nur von den personenbezogenen Daten der betroffenen Person zur Verfügung zu stellen.
Gleichzeitig darf nach Art. 15 Abs. 4 DS-GVO die Erfüllung des Rechts auf Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Nach dem Erwägungsgrund 63 erstreckt sich dieses Recht auch auf Geschäftsgeheimnisse, das Recht an geistigem Eigentum, insbesondere das Urheberrecht an Software. Damit sind auch die Rechte und Freiheiten juristischer Personen geschützt. Dies zugrunde gelegt, könnte man Art. 15 Abs. 3 DS-GVO so verstehen, dass dem Betroffenen lediglich eine Kopie aller seiner persönlichen Einzeldaten zur Verfügung zu stellen ist. Dies würde allerdings in vielen Fällen Art. 12 Abs. 1 DS-GVO zuwiderlaufen, der das Gebot der Verständlichkeit postuliert. Nach Auffassung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist das geschilderte Spannungsfeld wie folgt aufzulösen:
Der betroffenen Person sind alle Informationen nach Art. 15 Abs. 1 DS-GVO zur Verfügung zu stellen. Gleichzeitig besteht Anspruch auf eine Auskunft über die verarbeiteten personenbezogenen Daten des Betroffenen. Es besteht grundsätzlich kein Anspruch auf Kopie aller zu einem Betroffenen vorhandenen Datensätze aus sämtlichen Systemen. Zumindest ist ein Überblick zu gewähren, welche Daten in welchen Systemen verarbeitet werden. Die Bereitstellung kann dann verweigert werden, wenn Rechte und Freiheiten anderer Personen beeinträchtigt werden. Jedenfalls sind dem Betroffenen seine systemspezifischen persönlichen Stammdaten mitzuteilen sowie die ansonsten zu dieser Person gespeicherten oder sonst verarbeiteten Daten. Zur Verfügung zu stellen ist eine Liste dieser persönlichen Daten.

2.6 Datenschutz-Folgenabschätzung

Mit der Datenschutz-Grundverordnung (DS-GVO) wurde die bisherige Vorabkontrolle nach § 4d Abs. 5 Bundesdatenschutzgesetz alte Fassung obsolet und durch das neue Instrument der Datenschutz-Folgenabschätzung (DS-FA) nach Art. 35 DS-GVO ersetzt. Im Unterschied zur Vorabkontrolle ist die DS-FA aufgrund ihres risikobasierten Ansatzes in der Durchführung umfangreicher, methodischer und wird von einem DS-FA-Team durchgeführt. Aufgrund der vorherrschenden Unsicherheiten bei Thüringer Unternehmen in Bezug auf Notwendigkeit einer DS-FA und deren praktische Umsetzung, hat der TLfDI eine Handreichung zur DS-FA erstellt.

Mit der Datenschutz-Folgenabschätzung (DS-FA) verpflichtet die Datenschutz-Grundverordnung (DS-GVO) in Art. 35 Abs. 1 DS-GVO den Verantwortlichen vor einer Verarbeitung von personenbezogenen Daten, die voraussichtlich ein *hohes* Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Eine DS-FA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Durch den technikneutralen Ansatz des sachlichen Anwendungsbereiches der DS-GVO ist es ohne Belang, ob es sich um ein automatisiertes Verfahren oder um eine nichtautomatisierte Verarbeitung, zum Beispiel von Personaldaten in Papierakten, handelt.
Dabei ist zu beachten, dass die DS-FA kein einmaliger Vorgang ist. Wenn Risiken hinzutreten oder sich Verarbeitungsvorgänge oder auch der Stand der Technik grundlegend ändern, muss erneut eine DS-FA durchgeführt werden. Somit wiederholt sich der Prozess der Datenschutz-Folgenabschätzung zyklisch und ermöglicht somit eine kontinuierliche Überprüfung und gegebenenfalls Anpassung der Verarbeitung personenbezogener Daten.
Die formellen Anforderungen an eine DS-FA sind in Art. 35 der DS-GVO geregelt. Weiterhin finden sich Hinweise in den Erwägungsgründen 84 und 89 bis 93 der DS-GVO. Die Methodik der Durchführung wird in der DS-GVO nicht festgelegt. Hier besteht ein gewisser

Spielraum für die Verantwortlichen. Es ist jedoch ratsam, auf bestehende Methoden oder Standards zurückzugreifen. Ein Beispiel ist die Methodik nach dem Standard-Datenschutzmodell (SDM), siehe hierzu Punkt 5.26 des 1. Tätigkeitsberichts zum Datenschutz nach der DS-GVO, das in seiner neuen Version 2.0 abrufbar ist unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/sdm-methode_v2.0.pdf.

Gemäß § 38 Abs. 1 Bundesdatenschutzgesetz ist zu beachten, dass unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen immer ein Datenschutzbeauftragter zu benennen ist, wenn ein Verantwortlicher Verarbeitungen vornimmt, die einer DS-FA nach Art. 35 DS-GVO unterliegen.

Bevor eine DS-FA durchgeführt wird, ist in einem ersten Schritt zu klären, ob überhaupt eine Notwendigkeit zur Durchführung besteht. Bereits die Beantwortung dieser Fragestellung stellt eine Herausforderung für einige Thüringer Unternehmen dar, weshalb sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) entschloss, eine Handreichung zur DS-FA zu erstellen. Sie gibt dem Verantwortlichen ein Prüfungsschema an die Hand, mit welchem er prüfen kann, ob eine Notwendigkeit zur Durchführung einer DS-FA besteht. Auch wird darauf eingegangen, wer diese Vorprüfung durchführt.

Kommt der Verantwortliche in der Vorprüfung zu dem Ergebnis das eine DS-FA durchzuführen ist, gibt die Handreichung Hilfestellung bei der Durchführung der DS-FA. Dazu wird dargestellt, wer die DS-FA durchführt, welchen Umfang eine DS-FA hat und welche Schritte bei der Durchführung zu befolgen sind. Dabei werden insbesondere im Abschnitt Maßnahmen konkrete Beispiele und weiterführende Informationen zu technischen und organisatorischen Maßnahmen benannt. Auch die erstellten komprimierten grafischen Übersichten der Vorprüfung sowie des Gesamtprozesses der DS-FA sollen den Verantwortlichen durch die DS-FA lotsen.

Die Handreichung des TLfDI finden Sie unter https://www.tlfdi.de/mam/tlfdi/datenschutz/handreichung_ds-fa.pdf.

2.7 Datensicherheitsmaßnahmen gemäß DS-GVO

Verantwortliche haben gemäß Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) sicherzustellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“) ein. Diese Maßnahmen müssen regelmäßig überprüft und aktualisiert werden.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wird immer wieder gefragt, ob nach der Datenschutz-Grundverordnung (DS-GVO) überhaupt noch Datensicherheitsmaßnahmen, wie auch Log-Dateien beim Betreiben von Websites oder Ähnlichem rechtmäßig sind.
Gemäß Art. 24 Abs. 1 DS-GVO bestimmt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen müssen regelmäßig überprüft und aktualisiert werden.
Die Maßnahmen richten sich daran aus, dass die Sicherheit der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz gewährleistet werden. Die Ergebnisse vorgenommener Risikoanalysen gemäß Art. 32 Abs. 1 DS-GVO sind darin aufzunehmen, da sie Grundlage für die zu treffenden Maßnahmen sind.
Auch weisen die Grundsätze der Verarbeitung gemäß Art. 5 DS-GVO sowie die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DS-GVO eindeutig auf die Pflichten des Verantwortlichen hin. Dazu heißt es insbesondere in Art. 5 Abs. 2 DS-GVO: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht‘)“.

All dies führt – wie vor der Umsetzungspflicht zur Anwendung der DS-GVO auch – in direkter logischer Konsequenz zu einem entsprechenden Konzept, in der Praxis in der Regel als „IT-Sicherheitskonzept“ bekannt. Um die Forderungen der DS-GVO umzusetzen, gilt es also, die Gesamtheit der IT-Sicherheitsmaßnahmen sowie die Organisation der Sicherheit schlüssig zu dokumentieren.
Die Pflicht zur regelmäßigen Überprüfung und Anpassung ergibt sich aus Art. 32 DS-GVO, wonach 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 der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. In Art. 32 Abs. 1 Buchstabe d) DS-GVO wird dabei als eine mögliche Maßnahme ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung genannt. Ein mögliches Verfahren kann beispielsweise darin bestehen, zu bestimmten technischen Sachverhalten Log-Dateien zu erfassen und gezielt auszuwerten, um Reaktionen des Systems mit Bezug auf Soll-Zustände zu prüfen, Fehler zu beheben oder aber auch präventiv das Auftreten von Fehlern zu verhindern.
Aus Sicht des TLfDI gilt es dabei jedoch, das berechtigte Interesse, die Erforderlichkeit des Speicherumfangs und der Speicherdauer zu beachten. So unterliegt beispielsweise jegliche Datensicherheitsmaßnahme auch den Grundsätzen der Datenminimierung nach Art. 5 Abs. 1 Buchstabe c) DS-GVO. Daher gilt es stets auch das berechtigte Interesse einer Datenerhebung festzulegen und zu dokumentieren.
Zu beachten dabei ist, dass auch für alle anfallenden personenbezogenen Daten bei Datensicherheitsmaßnahmen die Zweckbindung gemäß Art. 5 Abs. 1 Buchstabe b) DS-GVO gilt.
Weiterhin ist zu regeln und zu dokumentieren, wer auf solche Datensätze von Datensicherheitsmaßnahmen mit personenbezogenen oder personenbeziehbaren Daten zugreifen darf, wer sie auswerten darf, wer wen bei einem Vorfall informiert beziehungsweise wer zu beteiligen ist und an wen welche Daten wann wie von wem weiterzugeben sind.

2.8 EuGH-Urteil zu Gmail

Der EuGH stellt klar, unter welchen Voraussetzungen ein internetbasierter E-Mail-Dienst einen „elektronischen Kommunikationsdienst“ nach derzeitigen Bestimmungen darstellt. Da der von Google erbrachte Dienst Gmail keinen Internetzugang vermittelt und nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht, gilt er nicht als ein derartiger Dienst.

Auslöser des Verfahrens war ein an Google gerichteter Bescheid der Bundesnetzagentur (BNetzA) von 2012, in dem die BNetzA den Dienst Gmail als Telekommunikationsdienst im Sinne von § 6 Abs. 1 Telekommunikationsgesetz (TKG) in Verbindung mit § 3 Nr. 24 TKG einordnete, weswegen Google der dort geregelten Meldepflicht gegenüber der BNetzA unterliege. Dagegen legte Google alle Rechtsbehelfsmöglichkeiten ein, mit der Begründung, Gmail sei kein Telekommunikationsdienst, da dieser Dienst keine Signale übertrage. Das bedeutet, Gmail ist ein sogenannter „Over-the-top-Dienst“ (OTT), ein über das Internet zur Verfügung stehender Dienst, ohne dass ein traditioneller Internet-Service-Provider involviert ist (Urteil des EuGH vom 13. Juni 2019 (Az. C-193/18, Rn. 10). Als reiner Webmail-Dienst setze Gmail zwar wie andere OTT-Dienste, etwa Online-Banking, eine Signalübertragung in diesem Sinne voraus, die Signalübertragung erfolge aber nicht durch Google selbst.
2018 wurde dann der Europäische Gerichtshof (EuGH) von dem derzeit für das Verfahren zuständigen Oberverwaltungsgericht München per Vorabentscheidungsersuchen um Klärung gebeten. Mit dem Urteil des EuGHs vom 13. Juni 2019 (Az. C-193/18) kam der EuGH nun zu dem Ergebnis, dass der E-Mail-Dienst Gmail tatsächlich nicht als „elektronischer Kommunikationsdienst“ im Sinne von Art. 2 Buchstabe c) der Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) (ABl. 2002, L 108, S. 21) in der durch die Richtlinie 2009/140 geänderten Fassung eingeordnet werden kann. Auch wenn Google als Betreiberin eigener Kommunikationsnetze elektronische Kommunikationsdienste erbringt, die der oben genannten Meldepflicht unterliegen, kann dies nicht dazu führen, dass sämtliche Dienste, die Google im Internet erbringt, auch als elektronische Kommunikationsdienste einzuordnen wären, obwohl sie nicht ganz oder überwiegend in der Über-

tragung von Signalen bestehen (Rn. 40). In Rn. 41 des EuGH-Urteils stellt das Gericht auch für andere E-Mail-Dienste klar, dass ein internetbasierter E-Mail-Dienst, der wie der von Google erbrachte Dienst Gmail keinen Internetzugang vermittelt, nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht, daher keinen elektronischen Kommunikationsdienst im Sinne dieser Bestimmung darstellt.

Das Oberverwaltungsgericht Münster hat nun in der Sache das Berufungsverfahren fortgesetzt und am 5. Februar 2020 entschieden, dass **Gmail kein Telekommunikationsdienst** ist. Eine Revision zum Bundesverwaltungsgericht (BVerwG) hat das Oberverwaltungsgericht nicht zugelassen. Hiergegen kann Beschwerde eingelegt werden, über die das BVerwG entscheidet (OVG 13 B 1494/19).

Das Urteil des EuGHs könnte allerdings bald überholt sein. Denn entsprechend der Richtlinie über den neuen europäischen Kodex für die elektronische Kommunikation (EKEK) müssen die Mitgliedstaaten bis zum 21. Dezember 2020 Rechts- und Verwaltungsvorschriften erlassen und veröffentlichen, die erforderlich sind, um dieser Richtlinie nachzukommen (Art. 124 EKEK, siehe Richtlinie (EU) 2018/1972: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972&from=EN). Diese Richtlinie beschäftigt sich unter anderem mit dem Begriff „elektronischer Kommunikationsdienst“.

Im Erwägungsgrund 15 dieser Richtlinie heißt es, dass, obwohl „Signalübertragung“ ein wichtiger Parameter für die Bestimmung der unter diese Richtlinie fallenden Dienste bleibt, die Begriffsbestimmung auch andere Dienste erfassen sollte, die Kommunikation ermöglichen. Aus der Sicht des Endnutzers spielt es keine Rolle, ob ein Anbieter die Signale selbst überträgt oder ob die Kommunikation über einen Internetzugangsdienst übermittelt wird.

Um einen wirksamen und gleichwertigen Schutz der Endnutzer und ihrer Rechte bei der Nutzung von in der Funktionsweise gleichwertigen Diensten zu gewährleisten, sollte eine zukunftsorientierte Definition von elektronischen Kommunikationsdiensten nicht allein auf technischen Parametern fußen, sondern eher auf einem funktionalen Ansatz aufbauen. So geht die Richtlinie davon aus, dass die Begriffsbestimmung für elektronische Kommunikationsdienste neben den

normalen Internetzugangsdiensten auch Interpersonelle Kommunikationsdienste beinhalten sollte. Interpersonelle Kommunikationsdienste sind Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch ermöglichen; dazu zählen Dienste wie herkömmliche Sprachanrufe zwischen zwei Personen, aber auch alle Arten von E-Mails, Mitteilungsdiensten oder Gruppenchats. Interpersonelle Kommunikationsdienste decken ausschließlich die Kommunikation zwischen einer endlichen – also nicht potenziell unbegrenzten – Zahl von natürlichen Personen ab, die vom Sender der Kommunikation bestimmt werden.
Gemäß Art. 2 Nr. 4 Buchstabe c) EKEK könnte ab dann Gmail doch als elektronischer Kommunikationsdienst gesehen werden. Der TLfDI wird über die Umsetzung in den einzelnen Mitgliedstaaten berichten.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat deshalb am 12. September 2019 den folgenden Beschluss „Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste“ gefasst:
„Auf Basis des Urteils des EuGH vom 13. Juni 2019 (Az. C –193/18) zur Auslegung des Begriffs des ‚Telekommunikationsdienste‘ gelten für die Zuständigkeitsverteilung zwischen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Aufsichtsbehörden der Länder vorbehaltlich einer Änderung der gesetzlichen Zuständigkeitsregelungen folgende Grundsätze:

1. Webmaildienste sind keine Telekommunikationsdienste im Sinne des Telekommunikationsgesetzes (TKG) in der derzeit geltenden Fassung. Dies gilt für reine Webmaildienste und für E-Maildienste, die zusammen mit einem Internetzugang angeboten werden, wenn die E-Mails (zumindest auch) über einen Webmailer abgerufen werden können. Daraus folgt, dass für die Datenschutzaufsicht mangels anderer besonderer Zuständigkeitsvorschriften allein die jeweiligen Landesdatenschutzaufsichtsbehörden zuständig sind. Die bisher beim BfDI geführten Verfahren werden an die jeweils zuständigen Landesaufsichtsbehörden zur Bearbeitung zuständigkeitshalber abgegeben.
2. Messenger-Dienste, die in einem geschlossenen System operieren, das heißt, bei denen die Nutzer/innen nur unter sich und nicht mit Nutzer/innen anderer Dienste kommunizieren können, können auch nach der genannten Entscheidung des EuGH als Telekommunikationsdienste im Sinne des TKG angesehen werden

mit der Folge, dass für diese Dienste weiterhin der BfDI aufsichtsrechtlich zuständig ist (§ 115 Abs. 4 TKG).“

(Quelle: https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zu_ott_diensten.pdf)

2.9 Positionspapier zur biometrischen Analyse

Anhand von Videoaufnahmen und der Auswertung des Gesichts einer Person können deren ungefähres Alter und Geschlecht recht zuverlässig bestimmt werden. Durch Analyse der Mimik sind zusätzlich auch Rückschlüsse auf die Gefühlslage eines Menschen möglich (sog. Emotional Decoding). Verantwortliche sind verpflichtet, die Grundsätze zu personenbezogenen Daten aus Art. 5 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) einzuhalten und die gemäß Buchstabe f) getroffenen Maßnahmen zu dokumentieren, Art. 5 Abs. 2 DS-GVO. Ergibt sich nach Durchführung der Risikoabschätzung die Pflicht zu einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO (Ergebnis der Abschätzung: „hohes Risiko“), ist die zuständige Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ damit beauftragt, sich gemeinsam mit dem Arbeitskreis „Videoüberwachung“ mit dem Thema der Verarbeitung von Daten durch Sensorik und Videotechnik und deren datenschutzrechtliche Einordnung zu befassen. Ziel des Auftrages war es, die Leistungsfähigkeit von biometrischen Sensoren einschließlich Videokameras und der dazu gehörigen Verarbeitungssysteme zu ermitteln, sowie Verarbeitungsziele und -prozesse zu beschreiben, rechtlich zu bewerten und Empfehlungen zur Gestaltung von Verfahren abzuleiten. Diese Analyse wurde im April 2019 von der 97. DSK als „Positionspapier zur biometrischen Analyse“ beschlossen. Das Positionspapier erläutert die Grundlagen der biometrischen Erkennung, stellt die Systeme zur Erfassung biometrischer Charakteristika dar, erläutert biometrische Sensoren, zeigt eine Sammlung möglicher Einsatzszenarien („Use Cases“) auf und kommt am Ende zur rechtlichen Bewertung. Daraus resultiert die Auswahl von Maßnahmen und

Schlussfolgerungen für die Verfahrensgestaltung. Da die Verarbeitung personenbezogener Daten immer ein Risiko für die Rechte und Freiheiten betroffener Personen darstellt, sind die Verantwortlichen dazu verpflichtet, die Grundsätze aus Art. 5 Datenschutz-Grundverordnung (DS-GVO) einzuhalten. Die getroffenen Maßnahmen sind nach Art. 5 Abs. 2 DS-GVO zu dokumentieren. Die Nicht-Einhaltung der in Art. 5 DS-GVO verankerten Grundsätze kann gemäß Art. 83 Abs. 5 Buchstabe a) DS-GVO mit einem Bußgeld geahndet werden. Zudem weist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit darauf hin, dass nach der Auswahl von technischen und organisatorischen Maßnahmen sowie deren Umsetzung das verbleibende Risiko für die betroffenen Personen beurteilt werden muss. Ergibt sich nach Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO ein hohes Risiko, muss die zuständige Aufsichtsbehörde konsultiert werden (Art. 36 DS-GVO)

https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/final_positionspapier-biometrie-v-1-0.pdf

Hinweise zur Datenschutz-Folgenabschätzung finden Sie in diesem Tätigkeitsbericht unter Nummer 2.6.

2.10 Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung

Welche Maßnahmen zu treffen sind, um nach dem aktuellen Stand der Technik einen sicheren Zugang zu Online-Diensten bereitzustellen, hat der Arbeitskreis Technik der DSK nun in seiner Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“ konkretisiert. Neben Anforderungen an die Eigenschaften von Passwörtern sowie ihre Übermittlung und ihre Verarbeitung, wird in der Orientierungshilfe klargestellt, dass bei einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen eine Zwei-Faktor-Authentifizierung auf Basis standardisierter Verfahren obligatorisch ist.

Anbieter von Online-Diensten, die personenbezogene Daten von Nutzerinnen und Nutzern verarbeiten, fallen unter die Regelungen der Datenschutz-Grundverordnung (DS-GVO). Sie haben insbesondere die Vorschriften zur Sicherheit der Verarbeitung (Art. 32 DS-GVO) zu

beachten. Hierzu gehören auch Maßnahmen zur Sicherung des Zugangs zu den Diensten. Die Auswahl und Implementation obliegt den Anbietern der Online-Dienste in eigener Verantwortung (Art. 24 DS-GVO).
Der Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in einer Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“ Maßnahmen beschrieben, die nach Ansicht der Datenschutzaufsichtsbehörden dem Stand der Technik entsprechen und einen effektiven Schutz gewährleisten können:
In Abhängigkeit der kryptographischen Speicherverfahren sind zum Beispiel in der Regel Passwortlängen von mindestens zehn Zeichen erforderlich, um von einem angemessenen Passwort mittlerer Güte zu sprechen. Zudem sollte sichergestellt sein, dass bereits kompromittierte Passwörter nicht erneut genutzt werden dürfen. Außerdem sind fehlgeschlagene Anmeldeversuche zu registrieren und es ist ein sicheres Passwort-Reset-Verfahren anzubieten. Passwörter sind vom Nutzer bei der Registrierung und Nutzung über einen, nach Stand der Technik kryptographisch abgesicherten, Transportkanal an den Endpunkt des Diensteanbieters zu übertragen. Anbieter dürfen zudem Passwörter nur nach Verarbeitung mittels kryptographischer Einwegverfahren (insbesondere [Salted-] Hashverfahren) nach dem Stand der Technik speichern. Eine Speicherung mittels symmetrischer Verschlüsselungsalgorithmen (zum Beispiel Advanced Encryption Standard – AES) ist in der Regel nicht notwendig und führt zu einem erhöhten Risiko, sollte der Verschlüsselungsschlüssel neben den verschlüsselten Daten entwendet werden. Weiterhin müssen die Anbieter die Datenbanken, in denen sie Nutzerpasswörter speichern, vor unbefugtem Zugriff durch eigenes Personal und Dritte sichern. Dazu sind regelmäßig unabhängige Penetrations- und Schwachstellentests durchzuführen.
Zusätzlich zum Passwortschutz soll eine Zwei-Faktor-Authentifizierung angeboten werden. Eine Zwei-Faktor-Authentifizierung ist bei Verarbeitungen mit hohem Risiko keine reine Empfehlung, sondern zum Erreichen eines angemessenen Schutzniveaus notwendig. Dabei sollen bevorzugt offene Verfahren wie Time-based One-time Password Algorithmus (TOTP) angeboten werden, also zeitlich limitierte Einmalpasswörter, welche nicht mit einer Offenbarung zusätzlicher personenbezogener Daten (Mobilfunknummern) verbunden sind.

Werden durch den Anbieter der Zwei-Faktor-Authentifizierung dennoch personenbezogene Daten wie Mobilfunknummern verarbeitet, sind geeignete Garantien anzubieten, welche eine Zweckbindung der Daten ausschließlich für die Zwei-Faktor-Authentifizierung dauerhaft sicherstellen. Weiterhin sollten standardisierte Verfahren wie beispielsweise WebAuthn unterstützt werden. WebAuthn ist ein Standard, mit dem Verantwortliche von Webanwendungen eine sichere Authentifikation des Nutzers anbieten können.

Sollte ein Anbieter davon Kenntnis erlangt haben, dass sein angebotener Dienst kompromittiert worden ist, so muss er entsprechend Art. 33 DS-GVO die zuständige Aufsichtsbehörde ohne zeitliche Verzögerung darüber informieren. Zudem sind geeignete Maßnahmen zu ergreifen, die dafür sorgen, dass Unbefugte mit diesen kompromittierten Informationen keinen Zugriff auf die Konten erhalten. Die Orientierungshilfe kann nachgelesen werden unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_anbieter_onlinedienste.pdf.

2.11 Windows 10

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat ein Prüfschema für den Einsatz von Windows 10 veröffentlicht. Das vorliegende Prüfschema soll Verantwortliche, die Windows 10 bereits einsetzen oder dies beabsichtigen, in die Lage versetzen, eigenständig die Einhaltung der rechtlichen Vorgaben der Datenschutzgrund-Grundverordnung (DS-GVO) in ihrem konkreten Fall zu prüfen und zu dokumentieren.

Im 3. Tätigkeitsbericht für den nicht-öffentlichen Bereich des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bereits über Windows 10 berichtet (Punkt 12.1, Seite 384). In den weiteren Untersuchungen durch die Aufsichtsbehörden rückte das Thema Telemetriedaten in den Fokus. Diese Daten werden durch Windows zu Analysezwecken erhoben und können unter Umständen personenbezogene Daten enthalten. Weiterhin besteht auch das Problem, dass die Betriebssystemdienste an Cloud-Services von Microsoft angebunden sind und diese Services auch Daten dorthin

übermitteln. Die Datenübermittlung geschieht vom Nutzer meist unbemerkt.
Inwieweit diese Datenübermittlung zulässig ist, war eine Problemstellung, der sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) angenommen hat. Man ist zu der Auffassung gelangt, dass eine Zulässigkeit vom Einzelfall abhängt und nicht pauschal beantwortet werden kann. In diesem Zusammenhang hat nun die 98. DSK ein Prüfschema für Windows 10 als Betriebssystem und zugehörige Anwendungslösungen veröffentlicht. Die Links zum Prüfschema und deren Anlage können Sie der Pressemitteilung des TLfDI *„DSK beschließt Prüfschema zu Windows 10!“* vom 11. November 2019 entnehmen: https://www.tlfdi.de/mam/tlfdi/presse/191111_presseinfo_windows.pdf

Das Prüfschema soll Verantwortliche, die Windows 10 bereits einsetzen oder dies beabsichtigen, in die Lage versetzen, eigenständig die Einhaltung der rechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) in ihrem konkreten Fall zu prüfen und zu dokumentieren. Es wird deutlich gemacht, dass es momentan nicht möglich ist, die Übermittlung von eventuell auch personenbezogenen Daten an Microsoft komplett zu unterdrücken. Daher muss jeder Verantwortliche die Zulässigkeitsprüfung für seine Einsatzzwecke selbst überprüfen und gegebenenfalls eigene Lösungen zum Schutz personenbezogener Daten implementieren – eine allgemeine Aussage zur Zulässigkeit oder Unzulässigkeit bezüglich des Einsatzes zu Windows 10 gibt es also nicht. Vielmehr kommt es auf den konkreten Einsatz im Einzelfall an.

Außerdem sollte die Zulässigkeitsprüfung für jede neue Version (welche für gewöhnlich mindestens einmal im Jahr installiert werden muss) wiederholt werden. Damit wird der Einsatz von Windows 10 und dessen Prüfung ein recht aufwendiger Prozess.
Der Erstellung eines Prüfschemas war ein Auftrag der DSK an den Arbeitskreis Technik vorrausgegangen, eine datenschutzrechtliche Positionierung zum Einsatz von Windows 10 zu erarbeiten und diese zur Grundlage eines weitergehenden, vom Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) zu koordinierenden Dialoges mit Microsoft zu datenschutzrechtlichen Fragestellungen zum Produkt

Windows 10 zu machen (siehe https://www.datenschutzkonferenz-online.de/media/dskb/20190403_positionierung_windows_10.pdf). Das BayLDA ist die zuständige deutsche Datenschutzaufsichtsbehörde für Microsoft Deutschland. Die DSK wird daher auch 2020 das Thema wieder aufgreifen, um mit Microsoft nach einer Lösung zu suchen, wie Windows 10 *einfach* datenschutzfreundlich einsetzbar wird.

2.12 Orientierungshilfe Telemedien

Verantwortliche von Websites sollten sich bewusstmachen, dass unzureichende oder pauschale Feststellungen, eine Datenverarbeitung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) sei zulässig, nicht die gesetzlichen Anforderungen erfüllen. Die Interessenabwägung im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO muss auf den konkreten Einzelfall bezogen sein. Sollte der Verantwortliche zum Ergebnis kommen, dass die Interessenabwägung zugunsten der betroffenen Person ausfällt und keine andere Rechtsgrundlage in Betracht kommt, ist die Datenverarbeitung – falls überhaupt – nur nach vorheriger informierter Einwilligung (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO) rechtmäßig.

Zur rechtlichen Bewertung der Einbindung von Analyse-Diensten auf Websites und Apps haben sich die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder im März 2019 in der „Orientierungshilfe für Anbieter von Telemedien“ auf ein gemeinsames Rechtsverständnis geeinigt. Die Orientierungshilfe gilt grundsätzlich für sämtliche Datenverarbeitungen durch Produkte und Dienste, derer sich Website- und App-Betreiber insbesondere auch zur Website-Analyse bedienen können: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf. Sie zeigt Beispiele auf und kommt im Ergebnis zu folgendem Fazit: *„Verantwortliche sollten sich bewusstmachen, dass die Interessenabwägung im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO)*

eine substantielle Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten verlangt und auf den konkreten Einzelfall bezogen sein muss. Unzureichende oder pauschale Feststellungen, dass eine Datenverarbeitung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zulässig sei, erfüllen nicht die gesetzlichen Anforderungen. Sollte der Verantwortliche zum Ergebnis kommen, dass die Interessenabwägung zugunsten der betroffenen Person ausfällt und keine andere Rechtsgrundlage in Betracht kommt, ist die Datenverarbeitung – falls überhaupt – nur nach voriger informierter Einwilligung (Art. 6 Abs. 1 Buchstabe a) DSGVO) rechtmäßig (‚jedenfalls dann...').“

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat in seiner Pressemitteilung vom 14. November 2019 (https://www.tlfdi.de/mam/tlfdi/presse/191114_pressemitteilung_zu_google_analytics.pdf) nochmals darauf hingewiesen: *„Wenn in Websites Dritt-Dienste, also z. B. Analyse-Tools, welche Daten über das Nutzungsverhalten betroffener Personen an Dritte weitergeben, eingebunden werden, deren Anbieter personenbezogene Daten auch für eigene Zwecke nutzen, ist das rechtlich nur noch zulässig, wenn zuvor eine Einwilligung der Nutzerinnen und Nutzer eingeholt worden ist. Zu solchen Diensten gehört auch Google Analytics.“* Der TLfDI prüft auch derzeit im Rahmen seiner Befugnisse eine Reihe von Internetauftritten von Thüringer Stellen auf die Einhaltung der DS-GVO.

2.13 Facebook-Fanpage

Die Konferenz der deutschen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) kam in einem Positionspapier am 3. und 4. April 2019 zum Ergebnis, dass ein datenschutzkonformer Betrieb einer Facebook-Fanpage derzeit weiterhin nicht möglich ist.

Bereits in Nummer 5.13 des 1. Tätigkeitsberichts zum Datenschutz nach DS-GVO 2018 positionierte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zu Facebook-Fanpages von Thüringer Stellen wie folgt:

„Sie werden daher gebeten zu prüfen, ob Sie die Informationspflichten nach der DS-GVO in Bezug auf die Fanpage gegenüber den betroffenen Personen erfüllen können. Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks. Daher müssen Sie dafür sorgen, dass Facebook Ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden. Dies betrifft alle in Art. 13 DS-GVO genannten Informationen. Auch muss mit Facebook eine Vereinbarung nach Art. 26 DS-GVO geschlossen werden. Angesichts der sehr deutlichen Entscheidung des EUGH rate ich dazu, die Fanpage zu deaktivieren. Sofern Sie davon Abstand nehmen, sollten Sie zumindest an den Verantwortlichen herantreten, um die nach Art. 13 DS-GVO erforderlichen Informationen zu erlangen und die nach Art. 26 DS-GVO notwendige Vereinbarung schließen zu können.“

Der TLfDI wurde auch dieses Jahr mehrfach gebeten, eine aktuelle datenschutzrechtliche Würdigung zum Betreiben von Facebook-Fanpages zu geben.

Bereits die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im Juni 2018 machte deutlich, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben (vergleiche hierzu https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/zwischenKonferenzen/entschliessung_dsk_fanpages_eugh_urteil_05_06_2018.pdf).

Diese Entschließung von der DSK aus dem Jahr 2018 wurde inhaltlich bei der Beratung des Gremiums am 3. und 4. April 2019 nochmal mit einem Positionspapier bestätigt: https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/final_positionierung_facebook_fanpages.pdf.

Die DSK ist der Meinung, dass die von Facebook veröffentlichten Informationen zu den Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO unterfallen, nicht hinreichend transparent und konkret dargestellt sind. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen. Die DSK erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

2.14 Google-Formular

Im Rahmen seiner Beratungstätigkeit wurde der TLfDI seitens einer öffentlichen Stelle angefragt, inwieweit die Nutzung von „Google Formulare“ als dienstliches Werkzeug zulässig ist. Eine Untersuchung ergab, dass es für öffentliche Stellen Bedenken hinsichtlich der Zulässigkeit der Nutzung gibt. Über dieses Ergebnis hat der TLfDI alle obersten Landesbehörden informiert.

Der Thüringer Landesbeauftrage für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von einer öffentlichen Stelle angefragt, inwieweit die Nutzung des Dienstes von „Google Formulare“ zulässig ist (siehe https://www.google.de/intl/de/forms/about/). Der Google-Dienst „Google Formulare“ ermöglicht es dem Nutzer, eigene Umfragen / Frageformulare zu erstellen, Umfragen durchzuführen und durch Google auswerten zu lassen. Grundsätzlich handelt es sich dabei um ein Instrument, dass auch für Aufgaben der öffentlichen Verwaltung genutzt werden könnte. Das Instrument ist dabei jedoch nur online über die Server von Google erreichbar. Eine Prüfung ergab, dass öffentliche Stellen diesen Google-Dienst momentan nicht einsetzen sollten, da es Bedenken hinsichtlich der Verarbeitungszwecke seitens Google gibt und auch die Datenverarbeitung selbst nicht deutlich genug erläutert wird (wie dies Art. 13 Datenschutz-Grundverordnung

[DS-GVO] fordert). Zur Erläuterung: Bei der Nutzung der Google-Dienste fallen personenbezogene Daten an, die Google für eigene Zwecke nutzt und welche auch für den Betrieb der Dienste nicht notwendig sind.
Daher hat der TLfDI in diesem Zusammenhang die obersten Landesbehörden Thüringens auf Folgendes hingewiesen:
„Der Dienst setzt einen Google Account voraus. Dabei anfallende personenbezogene Daten, die dazugehörigen Metadaten sowie Daten zum jeweiligen Inhalt und zu den verwendeten Elementen werden von Google erfasst. Es steht zu vermuten, dass die Daten auf eigenen Servern gesammelt und auf unbestimmte Zeit gespeichert werden, um Auswertungen von erstellten Umfragen vornehmen zu können. Der TLfDI kann nicht ausschließen, dass Google vollen Zugang zu allen Daten einer Umfrage hat und zudem die erfassten einzelnen Datensätze den Google-Nutzern zuordnen kann. Unklar ist in diesem Zusammenhang auch, wer Verantwortlicher für die Datenverarbeitung ist. Der TLfDI geht davon aus, dass die allgemeine Datenschutzerklärung (https://policies.google.com/privacy) für den Dienst Google Formulare gilt, da eine spezielle Datenschutzerklärung nicht bekannt ist. Nicht klar sind die Speicher- und Löschfristen und ob Google die gewonnenen Daten möglicherweise noch für andere Zwecke nutzt.

Die unklare Verantwortlichkeit, das Speichern jeglicher Google-Formulardaten zusammen mit einer mangelnden Transparenz hinsichtlich zusätzlicher Verarbeitungszwecke und Löschfristen haben zur Folge, dass der TLfDI von einer Nutzung dieses Google-Dienstes derzeit abrät. Ein DS-GVO-konformer Betrieb kann nur gewährleistet werden, wenn es der öffentlichen Stelle, die den Dienst einsetzt, gelingt, die dargestellten Unklarheiten aufzudecken und die Verarbeitung transparent zu machen. Dabei muss auch eine weitere Nutzung der Daten durch Google ausgeschlossen sein.“

2.15 Auch über den Clouds gibt es keine Datenschutz-Freiheit

Die Verarbeitung der Daten mittels weiterer Medien (beispielsweise Smartphone, Tablet oder via Internetbrowser über einen PC) ist datenschutzrechtlich von besonderer Bedeutung. Sollten Daten über eine

App in eine Cloud eingestellt werden, ist zum Beispiel der Betreiber einer Kamera für die Sicherheit der eingestellten Daten verantwortlich. Die Weitergabe der Daten an den Anbieter der Cloud ist nur dann rechtmäßig, wenn er mit diesem einen Vertrag zur Auftragsdatenverarbeitung geschlossen hat. Dieser Vertrag muss zumindest in Textform erfolgen und die im Einzelnen in Art. 28 Abs. 3 Datenschutz-Grundverordnung geregelten Punkte enthalten.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Beschwerde vor, dass eine Kamera womöglich auch öffentlich zugängliche Bereiche erfasse. Es stellte sich bei näherer Überprüfung heraus, dass der Kamerabetreiber den Eingangsbereich seines Grundstückes überwacht. Insoweit hat dieser einen Screenshot überreicht, auf dem dies zu erkennen war. Auf die Videoüberwachung weist der Kamerabetreiber mit einem Aufkleber am Briefkasten hin. Er hat zudem ein Verzeichnis von Verarbeitungstätigkeiten vorgelegt, wonach die Daten wöchentlich gelöscht werden. Bei der Kamera handelte es sich allerdings um ein Modell, bei dem die erhobenen Daten nicht beim Nutzer selbst (auf der Kamera / im lokalen Netzwerk auf einem anderen Speicher) gespeichert wurden, sondern in einer vom Hersteller bereitgestellten, online verfügbaren Speicherlösung, die über ein Benutzerkonto für den Kamerabetreiber zugänglich war.
Um die Bilder von der Kamera abzurufen, bieten die Hersteller eigene Apps für den jeweiligen Kameratyp an. Diese App verbindet sich direkt mit der Kamera, wenn der Nutzer sich im lokalen Netzwerk befindet. Viele Kamerahersteller ermöglichen aber auch den geschützten Zugriff auf die Bilder und Videos über das Internet. Diese Daten werden dann meist über Speichersysteme der Hersteller, den „Cloudspeicher“, abgerufen. Besteht zwischen dem Anwender und dem Betreiber des Speichersystems kein Auftragsverarbeitungsvertrag, müssen die Daten der Kamera zwingend im lokalen Netz gespeichert werden. Ein Zugriff auf diese Bilder und Videos über das Smartphone und/oder das Tablet ist über eine gesicherte Verbindung auch über das Internet möglich. Zum Teil ist es aber durch die Kamerahersteller nicht vorgesehen und nicht möglich, auf ein lokales Speichersystem zuzugreifen. In diesem Falle ist, wie oben bereits ausgeführt, die Weitergabe der Daten an den Betreiber des Speichersystems nur dann rechtmäßig, wenn er mit diesem einen Vertrag zur Auftragsdatenverarbeitung geschlossen hat. Dieser Vertrag muss zumindest in Textform erfolgen

und die im Einzelnen in Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) geregelten Punkte enthalten. Deshalb ist vor dem Kauf einer Kamera auf die rechtskonforme Verarbeitung der Daten zu achten. Nach der DS-GVO sind seitens der Verantwortlichen Speicherfristen einzuhalten. Hier gelten die Grundsätze des alten Bundesdatenschutzgesetzes (BDSG) insoweit weiter. Dies gilt auch vor dem Hintergrund von Art. 5 Abs. 1 Buchstabe c) DS-GVO, welcher die Datenminimierung, und Abs. 1 Buchstabe e) DS-GVO, der die Speicherbegrenzung vorsieht. Die zulässig durch die Überwachung gewonnenen Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen, Art. 17 Abs. 1 Buchstabe a) DS-GVO. Der TLfDI geht von einer Löschungsfrist von 48 Stunden aus. Nach Vortrag des Kamerabetreibers betrug die Speicherdauer bisher sieben Tage. Die Speicherfrist war daher auf höchstens zwei Tage zu reduzieren und entsprechend anzupassen.
Ebenso ist in dem vorgelegten Verzeichnis von Verarbeitungstätigkeiten die Speicherfrist entsprechend auf höchstens zwei Tage anzupassen. Der TLfDI bat daher, die Hinweise über die Videoüberwachung demgemäß zu überarbeiten und ihm ein entsprechend abgeändertes Verzeichnis vorzulegen, Art. 30 Abs. 4 DS-GVO.
Der TLfDI hatte dem Kamerabetreiber nochmals Gelegenheit gegeben, sich zu den hier getroffenen Feststellungen zu äußern.
Da der Kamerabetreiber aber zwischenzeitlich die Kamera nachweislich deinstalliert hatte, hat sich die Angelegenheit in datenschutzrechtlicher Hinsicht erledigt.

2.16 Meldungen nach Art. 33 – keine Angst vor Bußgeldern!

Die seit der Einführung der Datenschutz-Grundverordnung bestehende Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten, auch als „Datenpanne“ bezeichnet, wird von den Verantwortlichen in diesem Berichtszeitraum gegenüber dem vorherigen Berichtszeitraum vermehrt erfüllt, wenngleich wohl auch noch nicht vollständig.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum insgesamt 159 Meldungen zu Datenpannen. Die Meldungen der Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-

Grundverordnung (DS-GVO) lassen sich dabei in drei große Kategorien einteilen: Falschversendungen oder Kuvertierfehler, unbefugte Zugriffe auf Daten beziehungsweise systemkompromittierende Hackerangriffe sowie Fälle von Verlust oder Diebstahl von Daten. Aber auch Vorfälle, die das Versenden von Mails unter falscher E-Mail-Adresse (Identitätsdiebstahl) beinhalten, werden mitgeteilt. Hier ist allerdings unklar, ob wirklich eine „Datenpanne“ beim Verantwortlichen vorliegt oder nicht doch E-Mail-Adressen an anderer Stelle als beim Verantwortlichen ausgelesen wurden.
Der Anstieg der Meldehäufigkeit ist aus der Sicht des TLfDI erfreulich. Gleichzeitig ist davon auszugehen, dass immer noch ein erheblicher Teil an Datenpannen seitens der Verantwortlichen ungemeldet bleibt.
Der Angst vieler Verantwortlicher, dass sich aus der Meldung einer Datenpanne beim TLfDI ein Bußgeldverfahren zur Ahndung des Sachverhaltes, der die Datenpanne ausmacht, ergibt, kann an dieser Stelle entgegengetreten werden. Gemäß § 43 Abs. 4 Bundesdatenschutzgesetz (BDSG) darf eine Meldung nach Art. 33 DS-GVO in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder seine Angehörigen (entsprechend § 52 Strafprozessordnung) nur mit dessen Zustimmung verwendet werden. Gleiches gilt bei der Einleitung eines Strafverfahrens nach § 42 BDSG; auch hier darf nach § 42 Abs. 4 BDSG die Meldung nur mit Zustimmung des Meldepflichtigen verwendet werden. Mit diesen beiden Vorschriften soll das Verbot der Selbstbezichtigung gewahrt werden. Der Verstoß gegen die Meldepflicht an sich kann jedoch nach Art. 83 Abs. 4 Buchstabe a) DS-GVO mit einem Bußgeld geahndet werden. Aus diesem Grund ist die Meldepflicht nach Art. 33 DS-GVO bei „Datenpannen“ durch den Verantwortlichen in jedem Falle zu beachten.
Sofern von einer Meldung nach Art. 33 DS-GVO abgesehen wird, weil nach Bewertung und Einschätzung der Situation durch den Verantwortlichen kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, ist dies aufgrund des zuvor Gesagten stichhaltig zu begründen und sorgfältig zu dokumentieren.

3. Fälle öffentlicher Bereich

© alphaspirit – stressed spam – fotolia.com

3.1 Transparenz bei Online-Petitionen

Bei der Veröffentlichung von Online-Petitionen gilt: Gemäß § 14a Abs. 6 Thüringer Gesetz über das Petitionswesen werden bei der Veröffentlichung zusammen mit der Petition der Name und der Wohnort des Petenten sowie im Falle einer Mitzeichnung weiterer Petitionsberechtigter der Name und der Wohnort der Mitzeichnenden veröffentlicht.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine datenschutzrechtliche Frage zu einer Online-Petition, die auf der Website des Thüringer Landtags veröffentlicht wurde. Der Bürgerin, die an dieser Online-Petition teilnehmen wollte, fiel auf, dass bei einer Unterzeichnung der Petition der

Veröffentlichung von persönlichen Daten (Name und Wohnort) zugestimmt werden musste. Für die Bürgerin stellte dieser Umstand eine Einschränkung der Wahrnehmung ihres verfassungsmäßigen Rechts auf Teilnahme an einer Petition dar, da für sie keine Wahlmöglichkeit bestand, einer Veröffentlichung der personenbezogenen Daten zuzustimmen oder diese abzulehnen. Sie fragte also den TLfDI, ob die Verfahrensweise zur Veröffentlichung persönlicher Daten als Voraussetzung für die Unterzeichnung einer Online-Petition aus datenschutzrechtlicher Sicht gerechtfertigt sei.
Nach Prüfung des Sachverhalts konnte der TLfDI der Fragestellerin mitteilen, dass das Verfahren der Online-Petition aus datenschutzrechtlicher Sicht zulässig war. Petitionen sind Bitten oder Beschwerden, die in eigener Sache, für andere oder im allgemeinen Interesse vorgetragen werden. Ihre Handhabung wird im Thüringer Gesetz über das Petitionswesen (ThürPetG) geregelt. In § 14a ThürPetG werden speziell die „Petitionen zur Veröffentlichung“ geregelt. Diese sind definiert als Bitten oder Beschwerden von allgemeinem Interesse an den Landtag. Sie können auf Antrag des Petenten auf der Internetseite des Landtags veröffentlicht werden. Mit der Veröffentlichung erhalten auch weitere Petitionsberechtigte über das Internet die Gelegenheit zur Mitzeichnung der Petition. Allerdings ist diese Möglichkeit damit verbunden, dass bestimmte personenbezogene Daten ebenfalls veröffentlicht werden.
In § 14a Abs. 6 ThürPetG ist dabei vorgesehen, dass bei einer Veröffentlichung der Petition zusammen mit dieser der Name und der Wohnort des Petenten sowie im Falle der Mitzeichnung auch der Name und der Wohnort der Mitzeichnenden veröffentlicht werden.
Für die Transparenz und Nachvollziehbarkeit der Rechtmäßigkeit der Petition ist es wichtig, dass erkennbar wird, wer die Petition unterstützt. Eine Nicht-Veröffentlichung der persönlichen Daten würde dabei dem Sinn einer Online-Petition als demokratisches Beteiligungsinstrument entgegenstehen. Für die Veröffentlichung der genannten personenbezogenen Daten des Petenten und der Mitzeichnenden einer Online-Petition war somit eine Rechtsgrundlage vorhanden. Wer nicht möchte, dass seine personenbezogenen Daten veröffentlicht werden, muss sich nicht einer Online-Petition anschließen, sondern kann selbst eine „normale“ Petition einlegen. Damit liegt keine Einschränkung des Petitionsrechts vor.

3.2 Zentrales DMS

Behörden des Landes Thüringen haben gemäß § 16 Thüringer Gesetz zur Förderung der elektronischen Verwaltung (ab dem 1. Januar 2023 ihre Akten elektronisch in einem zentralen Verfahren zu führen. Das im Jahr 2017 gestartete Projekt „Zentrales DMS“, welches nun unter dem Namen „eAkte Thüringen“ geführt wird, dient dem Aufbau dieses zentralen Verfahrens. Der TLfDI ist seit Anbeginn beratend als Anwender und in seiner Funktion als Aufsichtsbehörde im zentralen Steuerungsgremium tätig.

Wie bereits im 1. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2018 in Kapitel 5.3 berichtet, müssen die Behörden des Landes Thüringen gemäß § 16 Thüringer Gesetz zur Förderung der elektronischen Verwaltung (ThürEGovG) ab dem 1. Januar 2023 ihre Akten elektronisch in einem zentralen Verfahren führen. Das im Jahr 2017 gestartete Projekt „Zentrales DMS“, welches nun unter dem Namen „eAkte Thüringen“ geführt wird, dient dem Aufbau dieses zentralen Verfahrens. Das Projekt „eAkte Thüringen“ hat als Ziel, ein zentrales Verfahren für die Führung elektronischer Akten in Thüringer Behörden bereitzustellen. Grundlage des Verfahrens bildet dabei ein Dokumentenmanagementsystem (DMS), welches bereits beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bei weiteren Thüringen Behörden im Einsatz ist. Im Projekt werden neben technischen Anforderungen an die eAkte auch Standards in Bezug auf die elektronische Aktenführung und Organisation sowie den Datenschutz definiert.
Bereits zu Beginn des Projekts konnte der TLfDI, aufgrund seiner langjährigen Erfahrungen im Bereich der elektronischen Aktenführung, positiv auf die Ausgestaltung der Anforderungen an die eAkte und die datenschutzrechtlichen Anforderungen Einfluss nehmen. So wurde erreicht, dass im Projekt ein generisches Datenschutzkonzept für die eAkte erstellt wird, welches von den Behörden an die jeweiligen Erfordernisse angepasst werden kann. Aufgrund der in der eAkte verarbeiteten personenbezogenen Daten sowohl von Bürgern als auch Mitarbeitern der Landesbehörden, besteht aus Sicht des TLfDI ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen. Somit ist nach Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung (DS-FA) durchzuführen. Basierend auf den Empfehlungen des TLfDI soll eine DS-FA für die eAkte Thüringen durchgeführt werden,

welche die jeweiligen Behörden als Basis für ihre eigene DS-FA nutzen können.
Bei der Prüfung der vorgelegten Konzepte legte der TLfDI besonderes Augenmerk auf die Ausgestaltung der Anforderungen an die eAkte in Bezug auf die Langzeitspeicherung, Formatkonvertierung und Aussonderung. Dies dient dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO) sowie der Einhaltung der Bestimmungen zur Löschung (Art. 17 DS-GVO) und Einschränkung der Verarbeitung (Art. 18 DS-GVO) der DS-GVO.
Die Archivierung und Aussonderung gemäß dem Thüringer Gesetz über die Sicherung und Nutzung von Archivgut (Thüringer Archivgesetz -ThürArchivG-) vom 29. Juni 2018 (vergleiche Gesetz- und Verordnungsblatt für den Freistaat Thüringen, Nummer 8 – Tag der Ausgabe: Erfurt, den 26. Juli 2018) für „öffentliches Archivgut“ betrifft alle Ministerien, Behörden und Einrichtungen des Freistaats Thüringen und ist somit bei der Ausgestaltung der eAkte bereits in der Konzeption zu berücksichtigen. Für die eAkte soll eine Schnittstelle auf Basis des xdomea-Standards die Anbindung an das thüringische elektronische Magazin realisieren. Die hierfür notwendige Konvertierung der in der eAkte möglichen 5-stufigen Schriftgutstruktur (Akte-Teilakte-Vorgang-Teilvorgang-Dokument) in eine 3-stufige Struktur (Akte-Vorgang-Dokument) steht aus Sicht des TLfDI im Widerspruch zur in der DS-GVO geforderten Integrität bei der Verarbeitung personenbezogener Daten. Es besteht nach den derzeit vorliegenden Informationen die Gefahr, dass die Meta-Informationen der Teil-Akten und Teil-Vorgänge nach der Überführung verloren gehen.
Die Normen § 29 Thüringer Verwaltungsverfahrensgesetz, Art. 15 DS-GVO und § 20 des ThürEGovG bilden die Rechtsgrundlage für die Auskunft aud der eAkte. Der TLfDI setzte sich dafür ein, dass in der eAkte ein vollständiger Aktendruck mit vollständiger, revisionssicherer Paginierung sowie ein auszugweiser Export von Schriftgutobjekten als PDF-Datei möglich ist. Für eine datenschutzgerechte Nutzung soll die Möglichkeit vorgehalten werden, beim Erzeugen des PDF-Dokuments personenbezogene Daten zu schwärzen.
Nachdem im Jahr 2019 die Anforderungen an die eAkte Thüringen erhoben und erste Konzepte erstellt wurden, steht für das Jahr 2020 der Abschluss der Konzeptphase an. Die Erstellung der noch ausstehenden Konzepte sowie die Pilotierung der eAkte Thüringen und Konzepterprobung wird der TLfDI begleiten.

3.3 Alles richtig bei der Richtlinie zur Aufbewahrung von Akten und sonstigem Schriftgut in der Thüringer Verwaltung?

„Viel aufbewahren hilft viel“ – dieser Fehlschluss hat im Archivrecht und seiner Ausgestaltung im öffentlichen Dienst nichts zu suchen. Vielmehr hat die öffentliche Verwaltung ihre Unterlagen unter Berücksichtigung des Verhältnismäßigkeitsprinzips nur so lange aufzubewahren, wie dies unbedingt erforderlich ist. Diese Aufbewahrungsfristen sind nach Auffassung des TLfDI und unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts in jedem Fall in gesetzlichen Regelungen zu konkretisieren.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist nicht nur für die datenschutzrechtlichen Fragen und Beschwerden der Bürgerinnen und Bürger da, er nimmt auch Stellung zu Gesetzentwürfen, Verordnungen und Richtlinien, wenn ihn die Thüringer Landesverwaltung darum bittet.
Im Frühjahr 2019 legte das Thüringer Ministerium für Inneres und Kommunales (TMIK) die Neufassung der „Richtlinie über die Aufbewahrung von Akten und sonstigem Schriftgut in der Verwaltung des Freistaats Thüringen“ zur datenschutzrechtlichen Prüfung vor. Dieses Regelwerk legt für alle Landes- und Kommunalbehörden allgemeinverbindliche Aufbewahrungsfristen für deren Schriftgut fest. Die Richtlinie konkretisiert damit § 14 Abs. 1 des Thüringer Archivgesetzes, der allgemein bestimmt, dass die genannten öffentlichen Stellen die bei ihnen entstehenden Unterlagen innerhalb der durch Rechts- oder Verwaltungsvorschriften vorgegebenen Aufbewahrungsfristen zu verwahren und zu sichern haben.
Der TLfDI monierte in seiner ersten Stellungnahme, noch vor der sogenannten Ressortabstimmung zwischen den Ministerien, zur genannten Richtlinie insbesondere, dass die vorgesehenen Aufbewahrungsfristen von zum Teil zehn Jahren deutlich zu lang bemessen seien. Eine solche zehnjährige Aufbewahrungsfrist sah der Entwurf der Richtlinie zum Beispiel für Brieftagebücher sowie Posteingangs- und -ausgangsbücher (Nr. 1.8 der Anlage Aufbewahrungsfristen), für Unterlagen von Bund-/Länder-Gremien (Nr. 1.14 der Anlage Aufbewahrungsfristen) sowie für Unterlagen von geschichtlicher Bedeutung, insbesondere Vorarbeiten zur Verfassungsgesetzgebung (Nr. 5.1 der Anlage Aufbewahrungsfristen) vor. Der TLfDI wies deshalb darauf

hin, dass die Aufbewahrungsfristen erst mit dem Abschluss der öffentlichen Aufgabe zu laufen beginnen und bat daher das TMIK, unter Berücksichtigung des Verhältnismäßigkeitsprinzips und des hier zu beachtenden Grundsatzes der Erforderlichkeit zu prüfen, ob die Aufbewahrungszeit von zehn Jahren nicht zu lang bemessen sei.
Diesen datenschutzrechtlich berechtigten Einwänden des TLfDI folgte das TMIK jedoch nicht, sondern es legte dem TLfDI im Sommer 2019 im Rahmen der Ressortabstimmung einen insoweit unveränderten Entwurf der genannten Richtlinie vor. Der TLfDI kritisierte deshalb in seiner Stellungnahme erneut die in manchen Fällen deutlich zu lang bemessenen Aufbewahrungsfristen und wies darüber hinaus noch auf Folgendes hin:
Bereits das Bundesverfassungsgericht habe in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1) darauf hingewiesen, dass Beschränkungen des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz einer verfassungsmäßigen gesetzlichen Grundlage bedürften, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für die Bürgerinnen und Bürger erkennbar ergäben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprächen. Ferner habe der Thüringer Gesetzgeber diese Vorgaben des Bundesverfassungsgerichts bei der Aufbewahrung von Schriftgut in der Thüringer Justiz hinreichend beachtet, indem er seinerzeit in § 26 Abs. 1 des Thüringer Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes eine Verordnungsermächtigung, unter anderem zur Bestimmung von Aufbewahrungsfristen, aufgenommen hat.
Aufgrund dessen gab der TLfDI dem TMIK die Empfehlung zu prüfen, inwieweit die anzuwendenden Aufbewahrungsregelungen auf der Grundlage eines materiellen Gesetzes – und nicht nur auf der Grundlage einer Richtlinie – zu treffen sind.
Leider blieb auch diese Empfehlung des TLfDI im TMIK ungehört, denn eine gesetzliche Regelung für eine Verordnungsermächtigung wurde weder von der Landesregierung noch von den Fraktionen des Thüringer Landtags in § 14 Abs. 1 des Thüringer Archivgesetzes eingefügt.
Der TLfDI wird daher diese Lücke verstärkt zum Anlass nehmen, um im Rahmen seiner Bearbeitung von datenschutzrechtlichen Beschwerden genau darauf zu achten, ob hier einerseits die Aufbewahrungsfristen im konkreten Einzelfall nicht zu lang bemessen waren und ob diese dem rechtsstaatlichen Gebot der Normenklarheit entsprochen haben.

3.4 Das lange Warten auf Auskunft

Unter den Voraussetzungen des § 42 Thüringer Datenschutzgesetz (ThürDSG) hat der Verantwortliche den betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob und welche Daten der betroffenen Person verarbeitet werden. Dabei setzt der Verantwortliche gemäß § 44 Abs. 2 ThürDSG die betroffene Person schriftlich darüber in Kenntnis, wie mit ihrem Antrag verfahren wurde. Auch über die Einschränkung oder das eventuelle Absehen von einer Auskunft hat der Verantwortliche die betroffene Person gemäß § 42 Abs. 5 ThürDSG schriftlich zu unterrichten. Seitens des Verantwortlichen ist sicherzustellen, dass die entsprechenden Geschäftsprozesse innerhalb der jeweiligen Dienststelle so ausgestaltet sind, dass diese es ermöglichen, die Anträge effektiv und möglichst zügig zu beantworten.

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er sich in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt sah. Er teilte mit, dass er bereits im Jahr 2017 Auskunft über die zu seiner Person gespeicherten Daten sowie deren entsprechende Löschung bei einer Thüringer Landespolizeiinspektion (LPI) beantragt hatte. Nachdem er von dort nach mehrmaligem Nachfragen keine Rückmeldung erhalten hatte, bat er den TLfDI um Hilfe.
Doch auch die Nachfrage des TLfDI bei der zuständigen LPI war zunächst nicht von Erfolg gekrönt. Erst nachdem der TLfDI die LPI sowie das Thüringer Ministerium für Inneres und Kommunales als zuständige Aufsichtsbehörden über den Sachverhalt informierte, wurde die um Stellungnahme gebetene LPI tätig. Inhaltlich teilte die LPI mit, dass der betroffene Bürger als Zeuge bei der Polizei gespeichert worden sei. Dies sei aufgrund einer Zeugenvernehmung geschehen. Zwar war der Antrag des Bürgers bereits im September 2017 bei der LPI eingegangen, jedoch erfolgte zu dem Vorgang aufgrund eines Bürofehlers, der dazu führte, dass der Vorgang als erledigt eingestuft wurde, keine weitere Sachbearbeitung. Im März 2018 kam es zu einer telefonischen Rücksprache der LPI mit dem Beschwerdeführer, der um eine Sachstandsmitteilung bat. In diesem Telefonat informierte die LPI den Beschwerdeführer über die noch nicht vorgenommene Sachbearbeitung. Mitte des Jahres 2018 löschte die LPI dann die entsprechenden Daten des Betroffenen. Der bis dato zuständige behördliche Datenschutzbeauftragte informierte den Betroffenen zwar telefonisch

darüber im September 2018, ein entsprechendes Schreiben der LPI wurde dem Betroffenen jedoch erst nach der Intervention des TLfDI im Januar 2019 zugesandt.
In der Analyse und Beurteilung des Gesamtvorganges wurden Mängel bei der Sachbearbeitung durch die LPI festgestellt. Nach der erfolgten Löschung der personenbezogenen Daten erfolgte zunächst keine schriftliche Information an den Betroffenen.
Um zukünftig eine termingerechte und rechtskonforme Sachbearbeitung von datenschutzrechtlichen Vorgängen zu gewährleisten, wurden nach der Intervention des TLfDI die Geschäftsprozesse in der entsprechenden LPI in Auswertung des konkreten Vorganges intensiv geprüft. Sie wurden mit dem zuständigen Datenschutzbeauftragten kritisch ausgewertet und neu geordnet. Dazu gehörte schlussendlich aber auch die Bestellung eines neuen behördlichen Datenschutzbeauftragten.

3.5 „Wer sitzt da neben dir?“ – Blitzerfotos von Beifahrern

Rechtsgrundlage für die Anfertigung von Bildaufnahmen zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr bei Verdacht eines Verkehrsverstoßes ist § 100h Abs. 1 Satz 1 Nr. 1 Strafprozessordnung in Verbindung mit § 46 Abs. 1 Ordnungswidrigkeitengesetz. Die Norm erlaubt die Anfertigung von Bildaufnahmen ohne Wissen des Betroffenen, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger Erfolg versprechend oder erschwert wäre.

Ein Bürger erhielt nach einer Geschwindigkeitsüberschreitung ein Blitzerfoto, auf dem nicht nur der Fahrer, sondern auch der Beifahrer unverpixelt zu sehen war. Deswegen wandte er sich mit einer datenschutzrechtlichen Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Um den Vorfall einer datenschutzrechtlichen Klärung zuzuführen, ersuchte der TLfDI zunächst die Bußgeldstelle um eine Stellungnahme. Diese teilte dem TLfDI mit, dass es sich um einen Fehler im Rahmen des Massenverfahrens bei der Auswertung von festgestellten Geschwindigkeitsverstößen gehandelt habe. Das Verfahren läuft wie folgt ab: Zur Auswertung und Bearbeitung derartiger Verstöße verwenden die Mitarbeiter der Filmauswertung der Zentralen Bußgeldstelle ein computergestütztes Programm. Zunächst muss im Arbeits-

verlauf der Bildbearbeitung eines jeden Verstoßes der Auswerter einen Rahmen um die Abbildung des Fahrers und des Kennzeichens platzieren, um die genauen Ausschnitts-Bilder zu bestimmen. Sind zusätzlich auf dem Gesamtbild andere Personen, wie zum Beispiel Beifahrer beziehungsweise weitere Fahrzeuge mit Personen und Kennzeichen zu erkennen, muss der Auswerter diese Ausschnitte auf dem Gesamtbild mittels der Funktion „Radiergummi“ verdecken.
In vorliegenden Fall hatte der Auswerter den Kennzeichenrahmen zwar positioniert, aber nicht im ausreichenden Maße verschoben, sodass er mittels der „Radiergummi“-Funktion Teile des Beifahrers nicht vollständig verdeckte.
Nach Aussage der Bußgeldstelle sei die Sachlage mit dem Bearbeiter besprochen und ausgewertet worden.
Der TLfDI bewertete den Sachverhalt wie folgt:
Grundsätzlich ist jede Anfertigung eines Beweisfotos ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung der abgebildeten Person. Nach Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen (ThürVerf) hat jeder Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen. Diese Rechte dürfen nach Art. 6 Abs. 3 Satz 1 ThürVerf nur aufgrund eines Gesetzes eingeschränkt werden.
Rechtsgrundlage für die Anfertigung von Bildaufnahmen zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr bei Verdacht eines Verkehrsverstoßes ist § 100h Abs. 1 Satz 1 Nr. 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG). Auch das Bundesverfassungsgericht (BVerfG) hat in seinem Beschluss vom 5. Juni 2010 eindeutig klargestellt, dass ein Eingriff in das Grundrecht im Falle von Blitzerfotos gerechtfertigt ist (BVerfG Az: BvR 759/10). § 100h Abs. 1 Satz 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG erlaubt die Anfertigung von Bildaufnahmen und damit eine Datenerhebung ohne Wissen des Betroffenen, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Vorliegend hat das BVerfG ausgeführt, dass das Interesse der Allgemeinheit an einem sicheren Straßenverkehr gegenüber dem Eingriff in die informationelle Selbstbestimmung überwiegt. Nach einem Urteil des Oberlandesgerichts (OLG) Oldenburg (Az.: 2 Ss OWi 20/15) gilt dies ausdrücklich auch für Beifahrer, obwohl diese nicht für den Verkehrsverstoß verantwort-

lich sind. Darüber hinaus führte auch das BVerfG aus, dass andere Personen gemäß § 100h Abs. 3 StPO nur betroffen sein dürfen, wenn dies unvermeidbar ist. Nach Auffassung des Senates (OLG) ist es unvermeidbar, dass bei Anfertigung eines Fotos im Rahmen einer Verkehrsüberwachungsmaßnahme auch der Beifahrer mit abgebildet wird und sieht damit die Anfertigung des Lichtbildes als durch § 100h Abs. 3 StPO gedeckt an.
Zu prüfen, inwieweit die Nichtverpixelung des Beifahrers zu einem Beweisverwertungsverbot im Rahmen ihres Bußgeldverfahrens wegen des Geschwindigkeitsverstoßes führte, oblag nicht der Zuständigkeit des TLfDI. Vielmehr ist der TLfDI nur befugt, Verstöße gegen datenschutzrechtliche Bestimmungen festzustellen. Das Erstellen des unverpixelten Fotos des Beifahrers und damit die Datenerhebung war im konkreten Fall datenschutzrechtlich nicht zu beanstanden. Nicht datenschutzkonform waren der Versand dieses Fotos und damit die Datenübermittlung an den Bürger. Der TLfDI hat die Bußgeldstelle darauf hingewiesen, nochmals die Mitarbeiter zum Vorgehen bei Schwärzung der Beifahrer oder anderer Fahrzeuge zu belehren.

3.6 Transparenz von Gerichtsverhandlungen – Öffentlichkeitsgrundsatz vs. Datenschutz

Nach § 169 Gerichtsverfassungsgesetz ist die Verhandlung vor dem erkennenden Gericht einschließlich der Verkündung der Urteile und Beschlüsse öffentlich. Ein Abfragen der personenbezogenen Daten der am Prozess Beteiligten im Beisein der Öffentlichkeit ist wegen dieses Grundsatzes der Öffentlichkeit von Gerichtsverhandlungen datenschutzrechtlich zulässig.

Im Berichtszeitraum bat eine Bürgerin den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung, ob das Abfragen der personenbezogenen Daten sowohl des / der Angeklagten als auch von Zeugen in öffentlichen Gerichtsverhandlungen datenschutzrechtlich zulässig ist.
In Art. 55 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) hat der europäische Gesetzgeber die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommene Verarbeitung von personenbezogenen Daten von der Aufsicht ausgenommen. Nach Erwägungsgrund Nr. 20 zur DS-GVO gilt dieses Gesetz zwar unter anderem für Tätigkeiten der Gerichte. Es sollten die Aufsichtsbehörden jedoch

nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein, um die Unabhängigkeit der Justiz bei der Wahrnehmung ihrer gerichtlichen Aufgaben zu wahren.
Auch der Thüringer Gesetzgeber hat in § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) geregelt, dass dieses Gesetz für die Verarbeitung personenbezogener Daten durch die Behörden, die Gerichte und die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentlichen Stellen) gilt. Aus § 2 Abs. 9 Satz 1 ThürDSG in Verbindung mit § 2 Abs. 9 Satz 2 ThürDSG ergibt sich aber, dass die Bestimmungen dieses Gesetzes über die Aufsichtsbehörde für die Gerichte nur gelten, soweit sie in Verwaltungstätigkeiten aktiv werden. Aufsichtsbehörde ist der TLfDI daher nur im Rahmen der Verwaltungstätigkeit der Gerichte. Er ist nicht für die Verarbeitung personenbezogener Daten durch die Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig.
Die mündliche Verhandlung ist eindeutig eine gerichtliche Tätigkeit der Justiz, keine Verwaltungstätigkeit. Sie unterliegt nicht der Kontrolle des TLfDI.
Unabhängig hiervon gilt:
Gemäß § 169 Abs. 1 Satz 1 Gerichtsverfassungsgesetz (GVG) ist die Verhandlung vor dem erkennenden Gericht einschließlich der Verkündung der Urteile und Beschlüsse öffentlich. Dieser Öffentlichkeitsgrundsatz, für den sich der Gesetzgeber bewusst entschieden hat, soll sicherstellen, dass eine Kontrolle des Prozesses und des Urteils durch die Bürger möglich ist. Eine „Geheimjustiz“ soll vermieden werden. Darum haben grundsätzlich jeder Interessierte sowie Journalisten Zugang zu den mündlichen Verhandlungen. Der Grundsatz der Öffentlichkeit von Gerichtsverfahren ist eine Prozessmaxime, die mit dem Unmittelbarkeitsprinzip und dem Mündlichkeitsgrundsatz zusammenhängt.
Es gibt aber auch Ausnahmen, das heißt Verhandlungen, in denen die Öffentlichkeit nicht zugelassen ist. Verhandlungen, Erörterungen und Anhörungen in Familiensachen sowie in Angelegenheiten der freiwilligen Gerichtsbarkeit sind nicht öffentlich (§ 170 Abs. 1 GVG). In Familiensachen stehen die Interessen der häufig (mit-)betroffenen Kinder oder der Ehegatten im Vordergrund. Ebenso finden Strafverhandlungen gegen Jugendliche ohne Publikum statt.

In öffentlichen Gerichtsverhandlungen werden daher datenschutzrechtliche Vorschriften nicht verletzt, wenn personenbezogene Daten von Angeklagten oder Zeugen abgefragt werden.

3.7 Ein Identitätsnachweis ist nicht in jedem Fall ein Muss

Steht die Identität des Auskunftssuchenden fest, bedarf es keines Identitätsnachweises. Im folgenden Fall war der Auskunftssuchende ein Bediensteter der Stelle, an die er sein Auskunftsersuchen richtete.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Beschwerde eines Betroffenen. Dieser teilte mit, dass er gegenüber der Thüringer Polizei sein Auskunftsrecht gemäß § 42 Thüringer Datenschutzgesetz (ThürDSG) wahrnahm. Danach hat der Verantwortliche den betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Die Polizeibehörde verlangte von dem Antragsteller eine einfache Kopie seines Personalausweises, um die Auskunftserteilung an einen unberechtigten Dritten zu vermeiden. In diesem Fall war es jedoch so, dass es sich bei dem Auskunftsersuchenden um einen Bediensteten der Thüringer Polizei handelte. In seinem Antrag teilte er gegenüber der betreffenden Polizeidienststelle mit, dass er regelmäßig dienstliche Post erhalte und er damit seinen Identitätsnachweis in Form einer Ausweiskopie nicht als erforderlich erachte.
Der TLfDI konnte in diesen Fall schnell weiterhelfen. Er bat die betreffende Polizeidienststelle um eine Stellungnahme, insbesondere dazu, aus welchem Grund der Identitätsnachweis hier erforderlich sei. Die Polizeidienststelle teilte daraufhin mit, dass ihr im Rahmen der bisherigen Antragsbearbeitung dieser Umstand nicht bekannt gewesen und aus dem Antragsschreiben des Polizisten auch nicht explizit hervorgegangen sei. Die Auskunft wurde ihm dann ohne Identitätsnachweis erteilt.

3.8 Auskunftsrecht = Akteneinsichtsrecht beim Notar?

Einen Anspruch auf Akteneinsicht oder persönliche Kenntnisnahme sieht die Datenschutz-Grundverordnung (DS-GVO) nicht vor. Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von

dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und die in Art. 15 Abs. 1 Buchstaben a) bis h) DS-GVO aufgeführten Informationen.

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ein Thüringer Notar ihm sein Auskunftsrecht nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) zur Haupt- und Nebenakte einer Urkunde verweigerte.
Um den Vorfall einer datenschutzrechtlichen Klärung zuzuführen, ersuchte der TLfDI zunächst den Notar um eine Stellungnahme zum Auskunftsersuchen nach § 21 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 15 DS-GVO. Der Notar führte gegenüber dem TLfDI aus, dass der Beschwerdeführer Beteiligter in einem Beurkundungsverfahren aus dem Jahr 2002 sei. Im Zusammenhang mit diesem Beurkundungsauftrag habe der Notar personenbezogene Daten erfasst und gespeichert. Als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten des Beschwerdeführers berief sich der Notar auf Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) DS-GVO in Verbindung mit dem notariellen Berufsrecht (insbesondere Bundesnotarordnung [BnotO], Beurkundungsgesetz [BeurkG], Dienstordnung für Notarinnen und Notare [DONot]). Weiterhin führte der Notar aus, dass er die mehrfach gestellten Auskunftsanträge über die personenbezogenen Daten des Beschwerdeführers seit 2002 bislang jedes Mal erfüllt habe. Nunmehr begehrte aber der Beschwerdeführer ein Einsichtsrecht in die notarielle Haupt- und Nebenakte zu dem Verfahren aus dem Jahr 2002 über seinen Auskunftsanspruch nach Art. 15 DS-GVO hinaus.
Daraufhin überprüfte der TLfDI den Sachverhalt datenschutzrechtlich. Im Ergebnis folgte der TLfDI der Argumentation des Notars. Ein Anspruch auf Einsicht in die Haupt- und Nebenakte ergibt sich nicht aus der DS-GVO. Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und die in Art. 15 Abs. 1 Buchstaben a bis h) DS-GVO aufgeführten Informationen. Hiernach besteht lediglich das Recht auf Auskunft und kein Einsichtsrecht. Einen An-

spruch auf Akteneinsicht oder persönliche Kenntnisnahme sieht die DS-GVO nicht vor.
Das Recht auf Einsicht in notarielle Unterlagen regelt vielmehr das Berufsrecht, hier § 51 BeurkG. Gemäß § 51 Abs. 3 BeurkG hat jede in § 51 Abs. 1 BeurkG aufgeführte Person das Recht auf Einsicht in die Urschrift. Als Beteiligter war der Beschwerdeführer berechtigt, die Urschrift einzusehen. Ein Recht auf Einsicht in die Nebenakte eröffnet § 51 BeurkG jedoch nicht und ist gesetzlich nicht geregelt. Auch in der Entscheidung des Bundesgerichtshofes vom 30. November 1989 Az.: BGH III ZR 112/88 heißt es, dass „sich das Recht auf Einsicht grundsätzlich auf die Urschrift derjenigen Urkunden beschränkt, von denen die in § 51 Abs. 3 BeurkG näher bezeichneten Personen Ausfertigungen oder Abschriften verlangen können. Jedenfalls bedürfte eine solche Einsichtnahme gleichfalls des Einverständnisses aller Beteiligten; anderenfalls würde die Schutzfunktion der Schweigepflicht des Notars außer Kraft gesetzt.“ Im Ergebnis kann jedenfalls die Einsicht in die Nebenakten nur gewährt werden, wenn alle Beteiligten den Notar von der Pflicht zur Verschwiegenheit befreien, § 18 Abs. 2 BNotO (vergleiche BGH DNotZ 1990, 392, 393).
Im Ergebnis konnte der TLfDI keinen datenschutzrechtlichen Verstoß feststellen. Den Antrag auf Auskunft nach Art. 15 DS-GVO hatte der Notar datenschutzkonform beantwortet.

3.9 Datenschutz bleibt Datenschutz – mit oder ohne Regelung des Thüringer Gesetzgebers zum Kommunalwahlrecht

Auch wenn die §§ 18 und 23 Thüringer Kommunalwahlordnung keine ausdrückliche Regelung enthalten, muss ein Stadtratskandidat bei bestehender Auskunftssperre im Melderegister gemäß § 51 Abs. 1 Bundesmeldegesetz im Rahmen der Wahl nicht seine private Hauptwohnanschrift öffentlich bekanntmachen. In diesem Ausnahmefall genügt die Angabe einer Erreichbarkeitsanschrift.

Im Vorfeld der Thüringer Kommunalwahlen am 26. Mai 2019 beschwerte sich ein Kandidat für den Stadtrat beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass seine private Hauptwohnadresse im Amtsblatt veröffentlicht werden sollte. Für ihn bestand eine Auskunftssperre im Melderegister nach § 51 Abs. 1 Bundesmeldegesetz (BMG). Hintergrund waren Besonderheiten sowohl seiner ehrenamtlichen als auch

seiner beruflichen Tätigkeit, sodass die Auskunft mit einem hohen Sicherheitsrisiko für ihn und seine Familie verbunden gewesen wäre. Er bat den TLfDI daher um Unterstützung.
Auf Nachfrage des TLfDI vertrat der Wahlleiter der zuständigen Stadtverwaltung trotz der bestehenden Auskunftssperre die Auffassung, sich an den Wortlaut des Thüringer Kommunalwahlgesetzes (ThürKWG) und der Thüringer Kommunalwahlordnung (ThürKWO) halten zu müssen. Nach § 23 Abs. 1 ThürKWO hat der Wahlleiter die eingereichten Wahlvorschläge mit den in § 18 Abs. 1 Nr. 1 und 2 ThürKWO bestimmten Inhalten öffentlich bekanntzumachen. In der Anlage 5 wird ausdrücklich „Hauptwohnung, Straße, Hausnummer, PLZ, Wohnort“ vorgegeben.
Grundsätzlich konnte der Wahlleiter den Einwand des Stadtratskandidaten nachvollziehen. Ihm war bekannt, dass § 38 Satz 4 der Bundeswahlordnung und § 36 Satz 4 der Thüringer Landeswahlordnung statt der Anschrift der Hauptwohnung eine Erreichbarkeitsanschrift ausreichen lassen. Deshalb hatte er eine Stellungnahme vom Thüringer Ministerium für Inneres und Kommunales (TMIK) eingeholt und auch erhalten. Das TMIK führte in seiner Stellungnahme an den Wahlleiter aus, dass die Eintragung einer gültigen Auskunftssperre nach § 51 Abs. 1 BMG als bundesrechtliche Vorgabe auch ohne eine ausdrückliche Regelung gleichermaßen im Rahmen der Thüringer Kommunalwahlen zu beachten sei. Zum Schutz der Interessen der Bewerberinnen und Bewerber sei deshalb in diesen Ausnahmefällen in der öffentlichen Bekanntmachung der Wahlvorschläge nach § 18 ThürKWG in Verbindung mit § 23 in Verbindung mit § 18 Abs. 1 Nr. 1 und 2 ThürKWO anstelle der Wohnanschrift eine Erreichbarkeitsanschrift zu verwenden. Die Angabe eines Postfachs genüge hingegen nicht.
Der Wahlleiter teilte dem TLfDI mit, dass er diese Auffassung des TMIK beachte und umsetze. Der Stadtratskandidat konnte seine Erreichbarkeitsanschrift statt seiner Wohnanschrift angeben.
Der TLfDI würde eine ausdrückliche Regelung im ThürKWG durch den Thüringer Gesetzgeber befürworten, um auch anderen Thüringer Wahlleitern eine eindeutige Handlungsgrundlage zu bieten. Nur so wäre sichergestellt, dass von einer Veröffentlichung der Hauptwohnanschrift im Falle einer Auskunftssperre im Melderegister nach § 51 Abs. 1 BMG tatsächlich immer abgesehen wird. Diese Anpassung im Kommunalwahlrecht ist jedoch leider bisher nicht geplant. Der TLfDI erinnert das TMIK aber immer wieder gern.

3.10 Adressen im Amtsblatt – rechtlich zulässig, aber datenschutzrechtlich fragwürdig

Die in Amtsblättern veröffentlichten Anschriften von Bewerbern, die als Wahlvorschläge zugelassen sind, sind aufgrund des Vorliegens einer Rechtsgrundlage aus datenschutzrechtlicher Sicht zulässig. Die generelle Erforderlichkeit der Adressangabe betrachtet der TLfDI als fragwürdig. Hier ist aber der Gesetzgeber gefragt.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Anfrage einer Bürgerin. Sie bat um Auskunft, ob im Amtsblatt die öffentliche Bekanntgabe der postalischen Adressen von Bewerbern, die als Wahlvorschläge für eine Gemeinderatswahl zugelassen sind, aus datenschutzrechtlicher Sicht rechtmäßig sei.
Der TLfDI konnte ihr hierzu mitteilen, dass gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) der Datenschutz-Grundverordnung (DS-GVO) eine Datenverarbeitung rechtmäßig ist, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Gemäß § 18 Thüringer Kommunalwahlgesetz (ThürKWG) hat der Wahlleiter die vom Wahlausschuss als gültig zugelassenen Wahlvorschläge und Listenverbindungen spätestens am 22. Tag vor der Wahl in ortsüblicher Weise öffentlich bekanntzumachen.
Diese öffentliche Bekanntgabe erfolgte im vorliegenden Fall im Amtsblatt. Die Angabe der Anschrift der Wahlvorschläge ergibt sich dabei aus § 14 Abs. 2 Satz 2 ThürKWG. Danach sind Bewerber in erkennbarer Reihenfolge in einem Wahlvorschlag unter Angabe ihres Namens und Vornamens sowie ihres Geburtsdatums, ihres Berufs und ihrer Anschrift aufzuführen. Die öffentliche Bekanntgabe der zugelassenen Wahlvorschläge – wozu auch die Anschrift der einzelnen Bewerber zählt – war folglich für die Erfüllung einer rechtlichen Verpflichtung nach § 18 ThürKWG zulässig.
Eine Veröffentlichung der Anschrift im Amtsblatt wäre dann nicht zulässig, wenn eine Auskunftssperre gemäß § 51 Bundesmeldegesetz (siehe auch Beitrag Nummer 3.9) vorliegen würde.
Auch wenn eine Veröffentlichung der Anschrift zulässig ist, so ist für den TLfDI aus datenschutzrechtlicher Sicht die Erforderlichkeit der Adressangabe dennoch als fragwürdig zu erachten. Abhilfe könnte der Gesetzgeber schaffen.

3.11 Auskunft ist nicht gleich Auskunft

Kommunen müssen bei einem Auskunftsersuchen nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) in jedem Fachamt der Kommunalverwaltung nachprüfen, ob über die betroffene Person personenbezogene Daten vorliegen. Allgemeine Auskünfte genügen nicht den Anforderungen des Art. 15 DS-GVO. So auch im nachfolgenden Fall.

Gleich wegen mehrerer Anliegen beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Nach seiner Auffassung gebe es in einer Kommune einiges zu bemängeln. So sei auf der Homepage der Kommune keine SSL-Verschlüsselung (= Secure Socket Layer-Verschlüsselung, bei der es sich um ein Verschlüsselungsprotokoll zur Datenübertragung im Internet handelt) vorhanden, auch würde es keinen Hinweis geben, dass personenbezogene Daten, die beim Aufrufen der Homepage gespeichert werden, auch an eine andere Internetseite übergeben werden, was jedoch der Fall zu sein schien. In Rundmails würden zudem persönliche Daten übertragen werden. So sollen alle Empfänger in das Feld „An“ eingefügt worden sein, anstatt in das Empfängerfeld „BCC“. Und zuletzt führte der Bürger in seiner Beschwerde auf, dass er von der Kommune eine unzureichende Auskunft über seine verarbeiteten personenbezogenen Daten erhalten habe.
Die Überprüfung der Beauskunftung nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) an den Bürger ergab, dass diese nicht den Anforderungen genügte: Unter anderem enthielt die Auskunft keine Information über die Dauer der Speicherung der personenbezogenen Daten. Denn die Kommune hatte dem Bürger neben einem Ausdruck seiner gespeicherten Daten aus dem Einwohnermeldeamt die zu seiner Person gespeicherten Daten in der Kämmerei sowie die gespeicherten Daten, die dem Hauptamt vorlagen, mitgeteilt. Das Auskunftsrecht nach Art. 15 DS-GVO ist jedoch viel umfassender. Die betroffene Person hat ein Recht, eine Auskunft über alle über sie verarbeiteten beziehungsweise gespeicherten personenbezogenen Daten sowie zu den Informationen gemäß Art. 15 Abs. 1 DS-GVO zu erhalten. Dabei handelt es sich um folgende Informationen:

– die Verarbeitungszwecke; die Kategorien personenbezogener Daten, die verarbeitet werden;

- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DS-GVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Werden zudem personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person gemäß Art. 15 Abs. 2 DS-GVO das Recht, über die geeigneten Garantien gemäß Art. 46 DS-GVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

Die Kommune hätte somit in jedem Fachamt der Kommunalverwaltung nachprüfen müssen, ob personenbezogene Daten über den Bürger verarbeitet worden sind beziehungsweise noch verarbeitet werden und hätte die oben aufgeführten Informationen mitteilen müssen. Allgemeine Auskünfte, wie etwa ein Ausdruck der gespeicherten Daten aus dem Einwohnermeldeamt, erfüllen somit nicht die Voraussetzungen des Art. 15 Abs. 1 und Abs. 2 DS-GVO. Im Zuge der Prüfung der Beschwerde folgte die Kommune dem TLfDI und holte eine Überprüfung der Beauskunftung nach. Diese ergab, dass tatsächlich neben dem Einwohnermeldeamt, der Kämmerei sowie dem Hauptamt noch in weiteren Fachämtern personenbezogene Daten über den Bürger verarbeitet worden sind beziehungsweise noch verarbeitet werden. In-

folgedessen erstellte die Kommune eine datenschutzkonforme Auskunft.
Da bis zum Redaktionsschluss zu den anderen Beschwerdevorwürfen noch keine abschließende Beurteilung aus datenschutzrechtlicher sowie -technischer Sicht erging, wird der TLfDI über den Ausgang in seinem nächsten Tätigkeitsbericht berichten.

3.12 Ratsinformationssysteme

Bei der Ausgestaltung von Ratsinformationssystemen ist neben den datenschutzrechtlichen Vorgaben insbesondere die Thüringer Kommunalordnung zu beachten. Dokumente mit personenbezogenen Daten dürfen nur elektronisch bereitgestellt werden, wenn deren Vertraulichkeit gewährleistet ist. Dies kann per Verschlüsselung erfolgen oder mit gesichertem webbasiertem Zugriff. Tonmitschnitte und Videomitschnitte von Gemeinderatssitzungen unterliegen ebenfalls strengen Vorgaben.

Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen zur Gestaltung von Ratsinformationssystemen. Aus datenschutzrechtlicher Sicht ist hierzu Folgendes zu beachten:
Einberufung, Tagesordnung und Beratungsunterlagen:
§ 35 Abs. 6 Satz 1 Thüringer Kommunalordnung (ThürKO) regelt, dass Zeit, Ort und Tagesordnung der öffentlichen Sitzungen spätestens am vierten Tag, bei Dringlichkeit am zweiten Tag vor der Sitzung ortsüblich öffentlich bekanntgemacht werden müssen. Zudem darf die Tagesordnung inhaltsbezogen keine personenbezogenen Daten beinhalten. Daher spricht nichts dagegen, den Gemeinderatsmitgliedern diese Informationen zeitgleich elektronisch bereitzustellen.
Für nicht-öffentliche Sitzungen gilt die öffentliche Bekanntgabe nur insoweit, als dadurch der Zweck der Nichtöffentlichkeit nicht gefährdet ist (§ 35 Abs. 6 Satz 2 ThürKO). Eine unverschlüsselte elektronische Übermittlung wäre also nur in diesen Fällen erlaubt.
Sind weitere Dokumente zur Sitzung für die Öffentlichkeit bestimmt, ist es auch üblich, Ratsinformationssysteme zu verwenden. Es gibt zum Beispiel Ratsinformationssysteme, in denen alle Sitzungseinladungen und „öffentlichen“ Dokumente für alle Interessierten ohne Beschränkung im Internet zugänglich sind. Voraussetzung dafür ist, dass

keine personenbezogenen Daten enthalten sind und die Veröffentlichung Interessen Dritter nicht entgegensteht, siehe zum Beispiel bei der Stadt Erfurt: https://buergerinfo.erfurt.de/bi/si0040.php.

Der TLfDI empfiehlt übrigens, bei der Nutzung von Webportalen dringend die in der technischen Richtlinie TR-02102-02 vom Bundesamt für Sicherheit in der Informationstechnik ausgesprochenen Empfehlungen umzusetzen. Dies bedeutet, die Transportverschlüsselung sollte mindestens TLS 1.2 und höher sein.

Zur vorgesehenen Schriftform: § 35 Abs. 7 ThürKO regelt, dass die vorgesehene Schriftform durch die elektronische Form ersetzt werden kann, wenn alle Mitglieder des Gemeinderats einverstanden sind und für die Übermittlung elektronischer Dokumente einen Zugang eröffnen. § 3a des Thüringer Verwaltungsverfahrensgesetzes findet entsprechende Anwendung. In Gemeinden, die einer Verwaltungsgemeinschaft angehören, kann die Schriftform nach den Sätzen 1 und 2 des § 35 Abs. 7 ThürKO nur dann durch die elektronische Form ersetzt werden, wenn die Verwaltungsgemeinschaft ebenfalls einen Zugang für die Übermittlung elektronischer Dokumente eröffnet hat.

Niederschriften von Sitzungen:

Es ist zu unterscheiden zwischen Niederschriften öffentlicher und nicht-öffentlicher Sitzungen.

Nach § 42 Abs. 3 Satz 1 ThürKO können die Mitglieder jederzeit die Niederschriften einsehen und sich Abschriften der Niederschriften über „öffentliche“ Sitzungen erteilen lassen. Gemäß § 42 Abs. 3 Satz 2 ThürKO kann die Geschäftsordnung neben der Einsichtnahme in die Niederschriften die Übersendung von Abschriften der Niederschriften über öffentliche Sitzungen an alle Mitglieder des Gemeinderates vorsehen. Hat der Gemeinderat entschieden, dass die Gründe der Geheimhaltung nach § 40 Abs. 2 Satz 2 ThürKO weggefallen sind, gilt § 40 Abs. 3 Satz 1 und 2 entsprechend.

Nicht geregelt ist die Art der Übersendung der Niederschrift der öffentlichen Sitzung. Der TLfDI geht davon aus, dass – sofern von der Papierform abgewichen wird – der Versand nur erfolgen darf, wenn die Voraussetzungen des § 35 Abs. 7 ThürKO erfüllt sind, das heißt, alle Mitglieder des Gemeinderats einverstanden sind und für die Übermittlung elektronischer Dokumente einen Zugang eröffnen.

Für Niederschriften der nicht-öffentlichen Sitzungen sieht die ThürKO derzeit keine Öffnungsklausel für jegliche Übersendung vor.
Beschlüsse:
§ 40 Abs. 2 ThürKO regelt, dass die in öffentlicher Sitzung gefassten Beschlüsse unverzüglich in ortsüblicher Weise öffentlich bekanntzumachen sind. Die in nicht öffentlicher Sitzung gefassten Beschlüsse sind in gleicher Weise bekanntzumachen, sobald die Gründe für die Geheimhaltung weggefallen sind; die Entscheidung hierüber trifft der Gemeinderat.
Spätestens mit der ortsüblichen Bekanntmachung spricht also nichts dagegen, den Gemeinderatsmitgliedern zur Vervollständigung ihrer Unterlagen den Beschluss auch einfach elektronisch per Mail zuzustellen.
Satzungen:
Gemäß § 21 Abs. 1 ThürKO sind Satzungen auszufertigen und öffentlich bekanntzumachen. Die Form der öffentlichen Bekanntmachung von Satzungen ist in der Hauptsatzung zu regeln. In der Hauptsatzung kann also geregelt werden, dass neben ortsüblichen Aushängen, auch rechtswirksame Beschlüsse im Internet zu veröffentlichen und den Gemeinderatsmitgliedern elektronisch zur Verfügung zu stellen sind.
Eine Anmerkung noch zu Tonmitschnitten und Videoaufzeichnungen von Gemeinderatssitzungen: Ton- und Videomittschnitte von Gemeinderatssitzungen durch den Gemeinderat sind grundsätzlich verboten, wenn sie nicht ausdrücklich erlaubt sind, indem alle Anwesenden zugestimmt/eingewilligt haben. Zudem ist der Zweck von Tonmitschnitten und Videoaufzeichnungen zu bestimmen. Daraus ergibt sich, dass die Tonmitschnitte nur für einen eindeutig festgelegten und legitimen Zweck (Erstellung von Wortprotokollen) erhoben werden dürfen, Art. 5 Abs. 1 Buchstabe. b) Datenschutz-Grundverordnung (DS-GVO). Die Daten dürfen auch nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden.
Mittels Tonaufzeichnungen von Gemeinderatssitzungen werden zudem personenbezogene Daten von anwesenden Personen (Ratsmitgliedern, geladenen und anderen Gästen) verarbeitet, die unter Umständen als besondere Kategorien personenbezogener Daten sogar unter den besonderen Schutz des Art. 9 Abs. 1 DS-GVO fallen. So fallen mit Bezug auf Art. 9 Abs. 1 DS-GVO auch möglicherweise Daten an, aus denen eine rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Die Verarbeitung dieser Da-

ten ist grundsätzlich untersagt. Art. 9 Abs. 2 DS-GVO regelt Ausnahmen. Für ein Wortprotokoll käme hier als Rechtsgrundlage nur Art. 9 Abs. 2 Buchstabe a) DS-GVO infrage, also mit einer ausdrücklichen Einwilligung der betroffenen Personen zu bestimmten Zwecken. Es kann per Geschäftsordnung geregelt werden, dass zum Zweck einer Anfertigung des Wortprotokolls der Sitzung oder zu einem bestimmten Tagesordnungspunkt ein Tonmitschnitt möglich ist, wenn von allen Anwesenden (Mitgliedern und allen Gästen) nachweislich das Einverständnis vor der jeweiligen Aufnahme explizit erteilt wurde. Versagt einer der Anwesenden die Einwilligung, dürfen keine Tonmitschnitte und Videoaufzeichnungen erfolgen.
Gemäß Art. 5 Abs. 1 Buchstabe e) DS-GVO dürfen personenbezogene Daten zudem nur so lange gespeichert werden, wie diese für den Zweck der Identifizierung einer betroffenen Person in Verbindung mit dem gesprochenen Wort erforderlich sind. Da die erforderlichen Informationen (Aussagen, Redebeiträge, Zwischenrufe) auch mit Zuordnung zu einer identifizierten Person in das Sitzungsprotokoll übertragen werden und das Sitzungsprotokoll per Abstimmung in seiner Richtigkeit bestätigt wird, ist ein weiteres Aufbewahren des Tonmittschnittes danach nicht mehr erforderlich.
Zudem ist zu regeln, dass nach Bestätigung der Niederschrift, die Aufzeichnung unwiderruflich zu löschen ist. Das Löschprotokoll ist allen Anwesenden, zumindest den Ratsmitgliedern, zugänglich zu machen.
Eine Aufbewahrung der Tonmitschnitte über den Zeitpunkt der Beschlussfassung hinaus würde einen Verstoß gegen die Grundsätze der rechtmäßigen Verwaltung darstellen, da keine der Voraussetzungen von Art. 6 Abs. 1 Buchstabe a) bis e) DS-GVO eine längerfristige Verarbeitung in Form der Speicherung dieser personenbezogenen Daten rechtfertigt.
Eine davon abweichende Verfahrensweise würde gegebenenfalls Sanktionen des TLfDI als zuständige Aufsichtsbehörde für den Datenschutz nach sich ziehen.

3.13 Offenbarung von Bürgerdaten in der Kfz-Zulassungsstelle

Die Bearbeitung von personenbezogenen Daten in Anwesenheit unberechtigter Dritter stellt einen Verstoß gegen datenschutzrechtliche Bestimmungen dar. Um eine unberechtigte Kenntnisnahme von personenbezogenen Daten auszuschließen, hat die verantwortliche Stelle geeignete technische und organisatorische Maßnahmen zu treffen.

Darüber hinaus gilt es zu beachten, dass festgestellte Datenschutzverletzungen, im Falle eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen, gemäß Art. 33 Datenschutz-Grundverordnung (DS-GVO) an den TLfDI zu melden sind und hierbei eine Benachrichtigung der Betroffenen gemäß Art. 34 DS-GVO zu prüfen ist.

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den Umgang mit personenbezogenen Daten in einer Kfz-Zulassungsstelle. Demnach sei es aufgrund der Einrichtung eines Großraumbüros möglich, diverse Kundenanliegen mitzuhören. Im Hinblick auf die dargelegte Raumsituation bat der TLfDI die verantwortliche Kfz-Zulassungsstelle um Stellungnahme. Hierzu teilte der Landkreis mit, dass die Sachbearbeiter zwar in einem Raum, jedoch abgetrennt voneinander säßen. Die Wartezone sei separat und über eine anonyme Nummernvergabe geregelt, sodass immer nur ein Bürger über die gezogene Nummer zum Sachbearbeiter aufgerufen wird. Des Weiteren sei auf Wunsch die Nutzung eines Einzelbüros möglich. Bei heiklen Fällen sei dies grundsätzlich vorgesehen. Ergänzend zu dieser Angelegenheit wurde dem TLfDI von der verantwortlichen Stelle eine Datenschutzverletzung gemäß Art. 33 der Datenschutz-Grundverordnung (DS-GVO) gemeldet. Grund hierfür war, dass derselbe Beschwerdeführer die Unterlagen eines vorherigen Kunden mitnahm. Die Ursache für das Offenliegen von Unterlagen war nach Angaben der Kfz-Zulassungsstelle die überobligatorische Arbeitsbelastung zu diesem Zeitpunkt. Grundsätzlich sei geregelt, dass nach Beendigung eines Bürgergespräches die Unterlagen in einer für den Bürger unzugänglichen Ablage aufbewahrt werden. Angesichts des festgestellten Datenschutzverstoßes kam die Kfz-Zulassungsstelle ihren Pflichten nach und meldete die Datenschutzverletzung fristgerecht an den TLfDI. Zeitgleich wurde der Betroffene über die Datenpanne gemäß Art 34 DS-GVO informiert.
In Anbetracht der Stellungnahme des Landkreises zur Umsetzung der Raumsituation und der vorgenommenen Meldung gemäß Art. 33 und 34 DS-GVO konnte der TLfDI die Angelegenheit als abgeschlossen ansehen. Jedoch wurde die verantwortliche Kfz-Zulassungsstelle darauf hingewiesen, ihre Mitarbeiter hinsichtlich ihrer Sorgfaltspflicht im Umgang mit personenbezogenen Daten im Rahmen einer jährlichen Unterweisung zu sensibilisieren.

3.14 Brisanter Prüfungsbericht des Thüringer Rechnungshofs

Brisante Prüfungsberichte nach § 7 Thüringer Prüfungs- und Beratungsgesetz des Thüringer Rechnungshofes verstoßen nicht gegen datenschutzrechtliche Bestimmungen und sind den kommunalen Vertretungen bekanntzugeben. Auch können diese gemäß § 10 Abs. 1 Nr. 7 Gesetz über den Thüringer Rechnungshof anonymisiert an Pressevertreter herausgegeben werden.

Im Berichtszeitraum hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage einer Stadtverwaltung erhalten. Diese wollte vom TLfDI wissen, inwieweit der Prüfungsbericht der überörtlichen Prüfung der Haushalts- und Wirtschaftsführung des Thüringer Rechnungshofs den kommunalen Vertretungen gemäß § 7 Abs. 1 Satz 4 Thüringer Prüfungs- und Beratungsgesetz (ThürPrBG) bekanntzugeben sei. Da der Prüfungsbericht Feststellungen enthält, die Rückschlüsse auf die handelnden Personen zulässt, stand die Befürchtung im Raum, dass sich dies nachteilig auf die betroffenen Personen auswirken könnte. Der Bericht sei zwar anonymisiert, jedoch seien aufgrund der geringen Größe der Stadtverwaltung Rückschlüsse nicht auszuschließen. Zudem bat die Stadtverwaltung den TLfDI um Prüfung der Zulässigkeit der Übermittlung des Prüfungsberichts seitens des Thüringer Rechnungshofs an einen Pressevertreter, da ein Pressevertreter bereits im Besitz des Prüfungsberichtetes war, obwohl dieser noch nicht dem Stadtrat bekanntgegeben worden war.
Die rechtliche Beurteilung der Bekanntgabe des Prüfungsberichts gegenüber dem Stadtrat stellte sich für den TLfDI wie folgt dar:
Der Prüfungsbericht soll sich gemäß § 6 Abs. 2 ThürPrBG auf die Feststellung der Tatbestände und Mängel und die daraus abzuleitenden Erkenntnisse und Vorschläge beschränken. Feststellungen von nicht wesentlicher Bedeutung sind möglichst durch mündliche Hinweise auszuräumen. Die finanzielle Leistungsfähigkeit ist am Maßstab der Gewährleistung der künftigen Aufgabenerfüllung und der Finanzplanung zu beurteilen; dabei sind die entsprechenden Ergebnisse interkommunaler Vergleiche besonders zu berücksichtigen. Bei der Abfassung des Prüfungsberichts sind die Bestimmungen des Datenschutzes zu beachten. Nach § 7 Abs. 1 ThürPrBG werden die Prüfungsberichte vom Rechnungshof unmittelbar nach Erstellung an den gesetzlichen Vertreter der geprüften Körperschaft oder seinen Vertre-

ter im Amt und an die Rechtsaufsichtsbehörde der geprüften Körperschaft übersandt. Das Gleiche gilt für Beratungen nach § 1 Abs. 4 ThürPrBG. Sofern mündliche Erörterungen stattfinden, ist der Rechtsaufsichtsbehörde Gelegenheit zur Teilnahme zu geben. Prüfungsberichte sind den kommunalen Vertretungen bekanntzugeben; mindestens eine Ausfertigung ist jeder Fraktion auszuhändigen. Grundsätzlich werden die Prüfungsberichte des Rechnungshofs in den Sitzungen des Gemeinderats thematisiert.

Die Thüringer Kommunalordnung (ThürKO) regelt im § 40 die Öffentlichkeit der Sitzungen der kommunalen Vertretung. Nach § 40 Abs. 1 ThürKO sind die Sitzungen des Gemeinderats öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder das berechtigte Interesse Einzelner entgegenstehen. Über den Ausschluss der Öffentlichkeit wird in nicht-öffentlicher Sitzung beraten und entschieden.

Weil dem TLfDI nicht bekannt war, inwieweit der Prüfungsbericht, trotz Beachtung des Datenschutzes, Rückschlüsse auf einzelne Mitarbeiter zulässt, empfahl der TLfDI der Stadtverwaltung, die Debatte über den Bericht zu verallgemeinern, sodass kein Personenbezug in der öffentlichen Sitzung hergestellt werden könne. Der TLfDI merkte jedoch an, dass, sollte die Debatte des Prüfungsberichtes in der öffentlichen Sitzung dahinführen, dass über einzelne Mitarbeiter und deren Personalangelegenheiten diskutiert werden solle, dies unter Ausschluss der Öffentlichkeit stattfinden müsse. Die Nichtöffentlichkeit der Sitzung wäre erforderlich, da dann das berechtigte Interesse Einzelner an der Öffentlichkeit der Sitzung entgegenstehen würde.

Hinsichtlich der Herausausgabe des Prüfungsberichtes an den Pressevertreter seitens der Pressestelle des Thüringer Rechnungshofes ergab die Prüfung Folgendes:

Der Thüringer Rechnungshof hat auf Nachfrage des TLfDI mitgeteilt, dass die Herausgabe des Prüfungsberichts über die überörtliche Prüfung der Haushalts- und Wirtschaftsführung an den Pressevertreter durch Entscheidung des Kollegiums gemäß § 10 Abs. 1 Nr. 7 Gesetz über den Thüringer Rechnungshof (RHG TH) erfolgt sei. Da der Bericht personenbezogene Daten enthält, sei dieser daher in anonymisierter beziehungsweise pseudonymisierter Fassung herausgegeben worden. Nicht anonymisiert seien unter der Rubrik „Allgemeine Angaben der Gemeinde“ Angaben aus allgemein zugänglichen Quellen zur gegenwärtigen Besetzung von Personalstellen gewesen, beispielsweise zum Bürgermeister der Stadtverwaltung. Der Thüringer Rech-

nungshof stellte in seiner Stellungnahme an den TLfDI klar, dass im Rahmen der Güterabwägung insoweit das öffentliche Interesse überwiege. Die Öffentlichkeit habe ein hohes Interesse an der Aufklärung der vorgefundenen Missstände.
Gemäß § 10 Abs. 1 Nr. 7 RHG TH entscheidet das Kollegium unter dem Vorsitz des Präsidenten in allen Angelegenheiten von grundsätzlicher oder sonst erheblicher Bedeutung sowie in Angelegenheiten, die ihm vom Präsidenten, einem anderen Mitglied des Rechnungshofs oder einem Senat zur Beschlussfassung vorgelegt werden. Das Kollegium entscheidet insbesondere über Auskünfte zu Prüfungsfragen gegenüber Landtag, Landesregierung und Presse. Diese werden jedoch nicht vor Abschluss des Prüfungsverfahrens erteilt. Über den Abschluss der Prüfung entscheidet der zuständige Senat.
Der TLfDI teilte der Stadtverwaltung daher mit, dass die Pressestelle des Thüringer Rechnungshofes rechtmäßig handelte. Der Thüringer Rechnungshof durfte somit den Prüfungsbericht an die Presse herausgeben.

3.15 Nur fit ans Steuer – auch aus datenschutzrechtlicher Sicht erlaubt

Die Verarbeitung personenbezogener Daten ist 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, § 16 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe e) 2. Variante in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) Datenschutz-Grundverordnung. Das kann bedeuten, dass bei bestimmten Erkrankungen die gesundheitliche Eignung zum Führen eines Fahrzeugs jährlich nachgewiesen werden muss.

Ein ehemaliger Berufskraftfahrer beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Reihe von Anordnungen der Fahrerlaubnisbehörde zur Eignung zum Führen der Fahrerlaubnisklassen der Gruppe 1 (Fahrzeuge bis 3,5 t und Motorräder). Da er nicht mehr in seinem früheren Job tätig sei, verzichtete der ehemalige Berufskraftfahrer nach Begutachtung und darauffolgender Empfehlung der Fahrerlaubnisbehörde bereits auf seine Fahrerlaubnis der Gruppe 2 (Klassen C,

C1, CE, C1E, D, D1, DE, D1E [zum Beispiel Lastkraftwagen, Busse] und die Erlaubnis zur Beförderung von Fahrgästen [FzF]). Trotzdem verlangte die Fahrerlaubnisbehörde weiterhin die Vorlage von Gesundheitsdaten in Form von jährlichen verkehrsmedizinischen Gutachten zu seiner Fahreignung der Gruppe 1 innerhalb einer kurzen Zeitspanne. Der ehemalige Berufskraftfahrer teilte mit, dass er seit einiger Zeit Diabetiker sei, aber seit Jahren unfallfrei am Straßenverkehr teilnehme. Seit 2017 sei er wegen seiner bestehenden Nierenerkrankung Dialysepatient. Seine Krankheit sei aber unter Kontrolle und er habe diesbezüglich angebotene Schulungen absolviert. Zudem sei seine Fahrtüchtigkeit mehrfach gutachterlich bestätigt worden. Deswegen hielt der ehemalige Berufskraftfahrer die Forderung der Fahrerlaubnisbehörde zur jährlichen Begutachtung zur Fahreignung der Gruppe 1 für unangemessen.
Der TLfDI wandte sich sowohl an die Fahrerlaubnisbehörde, nämlich an das zuständige Landratsamt, als auch an die zuständige Aufsichtsbehörde, das Landesverwaltungsamt. Auf Nachfrage des TLfDI führte das Landratsamt in Absprache mit dem zuständigen Fachamt aus, dass nach der Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnis-Verordnung, FeV) eine Fahrerlaubnis nur in Gebrauch genommen werden kann, wenn der Betroffene zum Führen von Fahrzeugen geeignet ist. Werden Tatsachen bekannt, die Bedenken gegen die körperliche oder geistige Eignung des Fahrerlaubnisinhabers in Form einer Erkrankung oder eines Mangels nach Anlagen 4, 5 oder 6 FeV begründen, ist die Behörde gemäß § 46 Abs. 3 FeV verpflichtet, die Überprüfung der Fahreignung durch geeignete Maßnahmen auf der Grundlage der §§ 11 bis 14 FeV zu veranlassen. § 11 Abs. 2 FeV sieht die Anordnung eines ärztlichen Gutachtens vor, wonach durch die Behörde bestimmt wird, durch wen das Gutachten zu erstellen ist.
Insbesondere wegen der bestehenden Nierenerkrankung und der damit verbundenen Dialysebehandlung des ehemaligen Berufskraftfahrers war nach Auffassung des Landratsamtes in diesem Fall eine jährliche Begutachtung durch einen Facharzt mit verkehrsmedizinischer Qualifikation zur Überprüfung der Fahreignungsvoraussetzungen für die Fahrerlaubnisbehörde erforderlich. Eine andere sinnvolle oder zumutbare Alternative als die Anordnung der jährlichen Begutachtung war nach Ansicht der Fahrerlaubnisbehörde hier nicht ersichtlich. Die sichere Teilnahme der Allgemeinheit am Straßenverkehr überwog – so das Landratsamt – hier als öffentliches Interesse gegenüber dem Inte-

resse des ehemaligen Berufskraftfahrers, sich nicht jährlich von einem Facharzt begutachten zu lassen.
Das Landratsamt begründete die sehr kurzen Zeitspannen, innerhalb derer die Fahrtüchtigkeit durch Gutachten nachgewiesen werden musste, damit, dass sich die zeitlichen Abfolgen der Gutachtenanforderungen sowie die Art der geforderten Eignungsnachweise aus der festgestellten Befundlage in den jeweils vorgelegten verkehrsmedizinischen Gutachten des ehemaligen Berufskraftfahrers ergeben haben. Außerdem handelte es sich bei den seit 2015 jährlich geforderten Einschätzungen um fach- und hausärztliche Stellungnahmen hinsichtlich Verlauf und Entwicklung der bei dem ehemaligen Berufskraftfahrer vorliegenden Erkrankung. Diese begründeten sich auf ein zuletzt vom ehemaligen Berufskraftfahrer vorgelegtes Gutachten eines ausgebildeten Verkehrsmediziners vom Jahr 2015, wonach auf seine Empfehlung hin regelmäßig fach- und augenärztliche Kontrollen zu fordern und der Behörde in jährlichen Informationen zu dokumentieren waren.
Im Ergebnis teilte der TLfDI dem ehemaligen Berufskraftfahrer mit, dass sowohl das Landratsamt als Fachbehörde als auch die Fachaufsichtsbehörde, also das Landesverwaltungsamt, zu dem datenschutzrechtlich korrekten Ergebnis kamen, dass die Anordnungen zur Vorlage von ärztlichen Gutachten der Fahrerlaubnisbehörde rechtmäßig waren und kein Fehlverhalten erkennbar war. Des Weiteren wurde bereits die Rechtmäßigkeit des Verwaltungsverfahrens gegenüber dem ehemaligen Berufskraftfahrer mit Urteil eines Verwaltungsgerichts und mit Beschluss des Thüringer Oberverwaltungsgerichts bestätigt.
Auch wenn es für den ehemaligen Berufskraftfahrer mit Sicherheit eine enorme Belastung darstellt, kam auch der TLfDI zu dem Ergebnis, dass insbesondere die jährliche Begutachtung und die damit verbundene Datenerhebung nach § 16 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit Art. 6 Abs. 1 Satz1 Buchstabe e) 2. Variante in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) Datenschutz-Grundverordnung datenschutzrechtlich zulässig ist. Danach ist die Verarbeitung personenbezogener Daten 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. Vorliegend erfolgte die Datenerhebung und -verarbeitung im öffentlichen Interesse. Dies ergibt sich insbesondere aus den Begutachtungsleitlinien zur Kraftfahreignung (Abschnitt 3.6.). Danach fordert das

Interesse der Allgemeinheit an einer verkehrssicheren Teilnahme von Patienten mit Nierenerkrankungen am Straßenverkehr außerdem, dass auch die verantwortliche Fahrerlaubnisbehörde durch regelmäßige Nachbegutachtung im jährlichen Abstand die notwendigen Kenntnisse als Entscheidungshilfe erhält. Aus Sicht des TLfDI konnte der Vorgang damit abgeschlossen werden.

3.16 Anwohnerparkplaketten während des Thüringentags

Im Vorfeld des Thüringentags gab eine Thüringer Kommune an berechtigte Anwohner Parkplaketten unter Vorlage des Personalausweises aus, damit diese in den festgelegten Zonen parken und fahren konnten. Eine Beschwerdeführerin sah sich dadurch in ihren Rechten verletzt. Die Vorlage des Personalausweises als Identitätsnachweis ist nach dem Personalausweisgesetz aus datenschutzrechtlicher Sicht zulässig.

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da sie ihren Personalausweis in einer Thüringer Kommune vorlegen musste, um eine Anwohnerparkplakette während des Thüringentags zu erhalten. Der TLfDI nahm sich der Beschwerde an.
Die Überprüfung des TLfDI ergab, dass die Thüringer Kommune im Vorfeld des Thüringentages im Rahmen ihrer ordnungsbehördlichen Funktion an berechtigte Anwohner Parkplaketten ausgab. Hierzu hatte die Thüringer Kommune mehrere verkehrsrechtliche Anordnungen erlassen, um den fließenden und ruhenden Verkehr während des Thüringentags aus Gründen der öffentlichen Sicherheit und Ordnung zu regeln. Um in den festgelegten Zonen fahren und parken zu dürfen, war eine Ausnahmegenehmigung – Anwohnerparkplakette – gemäß § 46 Abs. 1 Straßenverkehrs-Ordnung erforderlich. Die Thüringer Kommune wies in ihrem Amtsblatt darauf hin, dass Anwohner gegen Vorlage ihrer Fahrzeugpapiere oder ihres Personalausweises die Parkplakette bei der Thüringer Kommune abholen könnten.
Das Personalausweisgesetz (PAuswG) regelt im § 1 die Ausweispflicht beziehungsweise das Ausweisrecht. Gemäß § 1 Abs. 1 Satz 2 PAuswG muss der Personalausweis auf Verlangen einer zur Feststellung der Identität berechtigten Behörde nach § 2 Abs. 2 PAuswG vorgelegt werden und ihr ermöglichen, das Gesicht mit dem Lichtbild des Ausweises abzugleichen. Des Weiteren gilt nach § 14 Nr. 2 PAuswG:

Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises darf ausschließlich erfolgen durch öffentliche Stellen und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20 PAuswG. Gemäß § 20 Abs. 1 PAuswG kann der Inhaber den Ausweis bei öffentlichen und nicht-öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.
Die Thüringer Kommune konnte daher gemäß § 1 Abs. 1 Satz 2 PAuswG als Identitätsnachweis den Personalausweis verlangen. Da neben dem Personalausweis auch die Fahrzeugpapiere als Identitätsnachweis vorgelegt werden konnten, oblag es der Beschwerdeführerin gemäß § 14 Nr. 2 PAuswG in Verbindung mit § 20 Abs. 1 PAuswG selbst, die Art des Nachweises der Identität zu bestimmen. Der Nachweis der Identität war erforderlich, um zu überprüfen, ob die Anwohner berechtigt waren, in den festgelegten Zonen fahren und parken zu dürfen. Ein datenschutzrechtlicher Verstoß war somit nicht festzustellen, da es die nach Art. 6 Abs. 1 Satz 1 Buchstabe c) in Verbindung mit Abs. 3 Datenschutz-Grundverordnung in Verbindung mit § 1 Abs. 1 Satz 2, § 2 Abs. 2, § 14 Nr. 2 und § 20 Abs. 1 PAuswG erforderliche Rechtsgrundlage für die Datenerhebung gab. Der TLfDI teilte dies der Beschwerdeführerin mit.

3.17 Hilfssheriff on Tour

Nach § 66 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) hat ein Bußgeldbescheid Angaben zu den Beweismitteln zu enthalten. Zu den Beweismitteln gehören auch Zeugen der vorgeworfenen Tat. Diese Beweismittel sind möglichst genau, also mit Name und Anschrift, zu bezeichnen. Gleiches gilt auch für das Verwarngeldangebot (§ 56 OWiG).

Im Berichtszeitraum hat sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Beschwerdefall gegen das Ordnungsamt einer Stadtverwaltung beschäftigt. Folgender Sachverhalt lag der Beschwerde zugrunde:
Der Beschwerdeführer wollte vom TLfDI wissen, ob seine Angabe von Name und Anschrift als Anzeigenerstatter von Falschparkern im Verwarngeldverfahren als Zeugen-Beweismittel datenschutzrechtlich zulässig sei. Der Beschwerdeführer teilte dem TLfDI mit, dass er regelmäßig seit 2017 Halt- und Parkverstöße angezeigt habe, infolge dessen Verwarn- und Bußgeldverfahren eingeleitet wurden. Darauf-

hin sei er als Zeuge mit Name und Anschrift sowohl im Verwarngeldverfahren als auch im Bußgeldverfahren benannt worden.
Auf Nachfrage des TLfDI führte das Ordnungsamt der Stadtverwaltung aus, dass nach § 66 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) ein Bußgeldbescheid Angaben zu den Beweismitteln enthalten muss.
Zu den Beweismitteln gehören auch Zeugen der vorgeworfenen Tat. Diese Beweismittel sind möglichst genau zu bezeichnen. Das bedeutet, dass bei Zeugen der Name und die Anschrift anzugeben sind. Somit soll der Betroffene die Beweisbarkeit des Tatvorwurfs und die Erfolgsaussichten eines Rechtsmittels überprüfen können.
Die Vorgaben für den Bußgeldbescheid sind auch für das Verwarngeldangebot (§ 56 OWiG) aus den genannten Gründen zwingend anzuwenden. Durch das Verwarngeldangebot soll gerade im Bereich der Verstöße mit geringer Bedeutung (wie dies im Bereich der Halt- und Parkverstöße massenhaft der Fall ist) der Erlass eines Bußgeldbescheides vermieden und das Bußgeldverfahren durch Zahlung des Verwarngeldes zum Abschluss gebracht werden. Besonders bei den geringfügigen Verwarngeldangeboten wegen Halt- und Parkverstößen (Höhe 10,00 bis 35,00 Euro) sollte der Betroffene abschätzen können, ob er das angebotene Verwarngeld zahlt oder sich gegen die Verwarnung wendet und es auf den Erlass eines Bußgeldbescheides ankommen lässt, denn dieser bringt die Festsetzung von zusätzlichen Kosten in Höhe von mindestens 28,50 Euro mit sich.
Wegen eines eventuell folgenden Bußgeldverfahrens macht der Verzicht der Angabe auf persönliche Daten im Verwarngeldangebot ohnehin keinen Sinn. Insbesondere im Rahmen der Akteneinsicht (§ 49 OWiG, §§ 46 OWiG in Verbindung mit § 147 Strafprozessordnung), die auf Antrag nach einem Verwarngeldangebot gewährt werden muss, werden die persönlichen Daten des Anzeigenerstatters bekannt. Aus datenschutzrechtlicher Sicht war die Angabe des Namens sowie der Anschrift vom Beschwerdeführer als Anzeigenerstatter nicht zu beanstanden. Wenn die Ordnungsbehörde durch eine private Anzeige über eine mögliche Ordnungswidrigkeit unterrichtet wird, ist eine Überprüfung aufgezeigter Anhaltspunkte zunächst erforderlich. Ob anschließend ein behördliches Bußgeldverfahren eingeleitet wird, liegt grundsätzlich im Ermessen der Ordnungsbehörde, § 47 Abs. 1 OWiG. Nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) darf eine Ordnungsbehörde dabei personenbezogene Daten verarbeiten, „wenn diese Verarbeitung für die Aufgabenerfüllung zu den in

§ 31 ThürDSG genannten Zwecken (unter anderem die Verfolgung und Ahndung von Ordnungswidrigkeiten) erforderlich ist und keine spezielleren Regelungen in anderen Gesetzen vorgehen“. Der Vorgang war damit für den TLfDI abgeschlossen.

3.18 Hundesteueranmeldung – „Ein Hund oder kein Hund?“

Die Erhebung und Verarbeitung personenbezogener Daten des Vorbesitzers eines Hundes im Rahmen der Erhebung der Hundesteuer durch die Stadt Weimar ist auch ohne Einwilligung des Betroffenen rechtmäßig. § 12 Abs. 1 Satz 5 Hundesteuersatzung der Stadt Weimar verpflichtet den Hundehalter, den Beginn der Haltung im Gebiet der Stadt Weimar und Daten zum Vorbesitzer anzugeben. Diese Regelung verfolgt ein im öffentlichen Interesse liegendes Ziel, hier die ordnungsgemäße Erhebung der Hundesteuer.

Ein Bürger informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), dass die Stadt Weimar bei einer Hundesteueranmeldung die Hundehalter aufforderte, dem entsprechenden Antrag folgende Pflichtanlagen beizufügen: den Impfpass/Tierhalterausweis, aus dem Rasse, Alter, Geschlecht, Name, Fellfarbe und Chipnummer des Hundes hervorgehen sowie die Angabe der Herkunft des Hundes mit vollständiger Anschrift des Vorbesitzers. Diese Angaben sollten anhand eines Kaufvertrages/Überlassungsvertrages oder eines ähnlichen Dokuments nachgewiesen werden.
Auf Nachfrage des TLfDI teilte die Stadt Weimar mit, dass § 12 Hundesteuersatzung der Stadt Weimar (HStS) die Rechtsgrundlage zur Erhebung und Verarbeitung der Daten des aktuellen und des vorherigen Hundebesitzers sei. Nach § 12 Abs. 1 Satz 5 HStS sind bei der Anmeldung vom Hundehalter der Beginn der Haltung im Gebiet der Stadt Weimar und Daten zum Vorbesitzer anzugeben. Der Grund für diese Erhebung personenbezogener Daten lag aus der Sicht der Stadt Weimar darin, zu verhindern, dass Steuern verkürzt oder hinterzogen würden. Nur so könne vermieden werden, dass Hundehalter ihre Hunde steuerlich nicht anmelden und/oder vorsätzlich falsche Angaben über den tatsächlichen Beginn der Hundehaltung machen. Es gelte der Grundsatz der Gleichmäßigkeit der Besteuerung. Hundehalter, die den Beginn der Haltung nicht wahrheitsgemäß angeben, würden gegenüber Hundehaltern, die ihre Anmeldung ordnungsgemäß vorneh-

men, einen steuerlichen Vorteil erlangen. Somit war es nach Angabe der Stadt Weimar unabdingbar, die Daten des Vorbesitzers sowie das Übernahmedatum des Hundes durch den neuen Halter anzugeben und miteinander abzugleichen.
Wenn sich anhand der erhobenen Daten feststellen lässt, dass ein Hundehalter die Hundesteuer verkürzt oder hinterzieht, ermöglicht die Stadt Weimar dem Betroffenen vor Erlass eines Verwaltungsaktes eine persönliche Stellungnahme im Rahmen einer Anhörung gemäß § 91 Abgabenordnung (AO) beziehungsweise eine rückwirkende steuerliche Anmeldung.
Nach umfassender datenschutzrechtlicher Prüfung kam der TLfDI zu dem Ergebnis, dass die Erhebung der personenbezogenen Daten zum Vorbesitzer ohne die Zustimmung des Betroffenen durch die Stadt Weimar zulässig ist.
Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle in Thüringen ist nach Art. 6 Abs. 1 Satz 1 Buchstabe c) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 16 Abs. 1 Thüringer Datenschutzgesetz rechtmäßig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erfolgt.
Im vorliegenden Fall stützte sich die Verarbeitung auf die HStS der Stadt Weimar, welche DS-GVO-konform ist und damit höherrangigem Recht entspricht. Die Regelungen in der Satzung beschreiben klar und präzise die Verarbeitungsvoraussetzungen. Somit ist die Verarbeitung ihrer personenbezogenen Daten für die Bürgerinnen und Bürger vorhersehbar. Darüber hinaus verfolgt die HStS auch ein im öffentlichen Interesse liegendes Ziel, nämlich die ordnungsgemäße Erhebung der Hundesteuer. Sie erfüllt damit eine Kontroll-, Überwachungs- und Ordnungsfunktion. Diese Funktionen rechtfertigen die Verarbeitung der genannten personenbezogenen Daten.
Soweit die Stadt Weimar aber die Vorlage eines Kaufvertrages/Überlassungsvertrages oder ein ähnliches Dokument fordern würde, ergibt sich dies nicht aus der HStS. Danach sind nur Daten zum Vorbesitzer anzugeben. Die Vorlage solcher Dokumente ist daher nicht erforderlich.

3.19 Informationspflichten nach der DS-GVO im Bereich der Vollstreckungsabteilung

Eine datenschutzrechtliche Informationspflicht für den Empfänger personenbezogener Daten entsteht auch, wenn ein anderer Verantwortlicher diese Daten zuvor schon einmal erhoben und dabei Informationspflichten aus Art. 13 Abs. 1 und Abs. 2 Datenschutz-Grundverordnung (DS-GVO) zu erfüllen hatte. Der Empfänger übermittelter Daten erhebt diese Daten, indem er sie zielgerichtet entgegennimmt, um sie weiterzuverarbeiten. Er muss darum die betroffene Person nach Maßgabe von Art. 14 Abs. 1 bis 3 DS-GVO informieren.

Im Berichtszeitraum lag dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage zu Informationspflichten nach der Datenschutz-Grundverordnung (DS-GVO) im Vollstreckungsbereich eines Landratsamtes vor. Nach Angabe des Landratsamtes erhält die Vollstreckungsabteilung die personenbezogenen Daten der Schuldner aus dem automatisierten Verfahren für das Haushalts-, Kassen- und Rechnungswesen des Bundes (HKR-Verfahren). Diese Daten seien zuvor bereits von einem anderen Fachamt erhoben worden. Insofern ging das Landratsamt davon aus, dass dadurch den betroffenen Personen bereits eine Information gemäß DS-GVO über die Datenerhebung zugegangen und eine weitere Information nicht erforderlich sei. Außerdem sei es für die Vollstreckung zumeist erforderlich, sich die persönlichen und wirtschaftlichen Verhältnisse der Schuldner erklären zu lassen. In diesem Fall plante das Landratsamt, auf eine Information nach der DS-GVO zu verzichten, da im Vollstreckungsverfahren eine gesetzliche Grundlage, insbesondere der Mitwirkungsgrundsatz (vergleiche § 26 Abs. 2 Satz 1 Thüringer Verwaltungsverfahrensgesetz [ThürVwVfG] oder § 93 Abgabenordnung [AO]), Anwendung fände. Dieses Anliegen begründete das Landratsamt insbesondere mit dem Erwägungsgrund 62 der DS-DVO zu Art. 14 Abs. 5 Buchstabe c) DS-GVO: Danach erübrige sich die Pflicht, Informationen zur Verfügung zu stellen, wenn die betroffene Person die Information bereits habe, wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt sei oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweise oder mit unverhältnismäßig hohem Aufwand verbunden sei.

Schließlich bat das Landratsamt den TLfDI noch um Mitteilung, wie es sich mit den Informationspflichten der Verantwortlichen verhalte, wenn Daten über die Schuldner bei Dritten erhoben würden, zum Beispiel Sozialträger, Rententräger, aus dem Einwohnermeldeamtsportal usw., da es auch für diese Fälle gesetzliche Grundlagen für die Erhebung der Daten gäbe (§ 74a Zehntes Buch Sozialgesetzbuch [SGB X] oder das Gesetz zu Verbesserung der Sachaufklärung in der Verwaltungsvollstreckung). Auch in diesen Fällen beabsichtige das Landratsamt auf die Information gemäß DS-GVO zu verzichten.
Der TLfDI teilte auf die Anfrage Folgendes mit:
Nach seiner Ansicht handelt es sich bei der Ausnahme nach Art. 14 Abs. 5 DS-GVO um eine Regelung, die restriktiv auszulegen ist. Soweit sich das Landratsamt darauf berief, dass nach Art. 14 Abs. 5 Buchstabe a) DS-GVO die Informationspflichten entfallen würden, wenn und soweit die betroffene Person bereits über die Informationen verfüge, gelten nach Ansicht des TLfDI hier die gleichen Bestimmungen, wie bei dem wörtlich übereinstimmenden Art. 13 Abs. 4 DS-GVO. Danach entfällt die Informationspflicht, wenn die betroffene Person gerade über die mitzuteilenden Informationen verfügt. Der Informationsstand der betroffenen Person muss daher in Ausmaß, Genauigkeit und Klarheit jenen Informationen entsprechen, die der Verantwortliche der betroffenen Person zur Verfügung stellen ließ. Insbesondere ergibt sich alleine daraus, dass eine gesetzliche Regelung einer Behörde erlaubt, Daten bestimmter Kategorien zu Zwecken bestimmter Kategorien zu erheben, noch nicht, dass bekannt sein muss, dass eine Datenerhebung im Einzelfall auf dieser Regelung beruht. Die Behörde muss die betroffene Person daher gemäß Art. 14 Abs. 1 Buchstabe c) DS-GVO ausdrücklich darüber informieren, auf welche Rechtsgrundlage sie sich gerade für die konkrete Datenerhebung stützt und welchen einzelfallbezogenen konkreten Zweck sie damit verfolgt (vergleiche Bäcker in Kühling/Buchner, DS-GVO Art. 13, Rn. 84 und 85). Damit der Ausnahmetatbestand des Art. 14 Abs. 5 DS-GVO greift, muss als zweite Voraussetzung die betroffene Person auch über die mitzuteilenden Informationen verfügen. Das heißt, die Informationen müssen nachweislich so in ihrem Herrschaftsbereich vorhanden sein, dass die betroffene Person sie ohne Weiteres zur Kenntnis nehmen kann. Eine Informationspflicht des Verantwortlichen entsteht daher auch, wenn ein anderer Verantwortlicher die Daten zuvor schon einmal erhoben hat und dabei Informationspflichten aus Art. 13 Abs. 1 und Abs. 2 DS-GVO zu erfüllen hatte. Bedeutsam ist dies vor

allem für Datenübermittlung. Der Empfänger übermittelter Daten erhebt diese Daten, indem er sie zielgerichtet entgegennimmt, um sie weiterzuverarbeiten. Er muss darum die betroffene Person nach Maßgabe von Art. 14 Abs. 1 bis 3 DS-GVO informieren, insbesondere der betroffenen Person nach Art. 14 Abs. 2 Buchstabe f) DS-GVO mitteilen, aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen. Infolgedessen war auch die Vollstreckungsabteilung als Empfänger einer Datenübermittlung aus dem HKR-Verfahren grundsätzlich verpflichtet, der betroffenen Person die Informationen nach Art. 14 Abs. 1 bis Abs. 3 DS-GVO mitzuteilen. Soweit Ordnungswidrigkeiten verfolgt oder geahndet werden, ist jedoch nicht die DS-GVO anzuwenden, sondern es gelten die §§ 31 ff. Thüringer Datenschutzgesetz (ThürDSG). Aber auch hier sehen die §§ 40 und 41 ThürDSG grundsätzlich vor, dass der Betroffene über die Verarbeitung seiner Daten zu informieren ist und ihm zum Beispiel die Zwecke und die Rechtsgrundlage der Datenverarbeitung anzugeben sind.

Aber zurück zur Fallfrage des Landratsamtes: Auch die Bestimmung des Art. 14 Abs. 5 Buchstabe c) DS-GVO hilft in einem derartigen Fall nicht weiter. Nach dieser Bestimmung entfallen die Informationspflichten des Art. 14 DS-GVO nur, wenn und soweit eine Rechtsvorschrift die Erhebung oder (zweckändernde) Offenlegung bestimmter Daten „ausdrücklich“ regelt. Dies setzt voraus, dass die Rechtsvorschrift hinsichtlich ihres Informationsgehalts für die betroffene Person eine Mitteilung durch den Verantwortlichen zumindest annähernd gleichwertig ersetzt. Eine ausdrückliche Regelung im Sinne von Art. 14 Abs. 5 Buchstabe c) DS-GVO besteht nur, wenn eine Rechtsvorschrift zumindest die Art der erhobenen Daten, die Voraussetzungen der Datenerhebung oder Offenlegung und den Verarbeitungszweck hinreichend spezifisch und normenklar vorgibt. Den Hauptanwendungsfall von Art. 14 Abs. 5 Buchstabe c) DS-GVO bilden gesetzliche Meldepflichten an Behörden, etwa zur Geldwäschebekämpfung oder zur ordnungsgemäßen Berechnung von Steuern oder Sozialversicherungsbeiträgen. Hier wird die Behörde, welche die Daten empfängt, von den Informationspflichten aus Art. 14 Abs. 1 und Abs. 2 DS-GVO freigestellt.

Wenn die Empfänger-Behörde die von ihr erhobenen Daten allerdings im Anschluss zweckändernd weiterverarbeitet, ist sie grundsätzlich nach Art. 14 Abs. 4 DS-GVO zur Information der betroffenen Person verpflichtet. Soweit das Landratsamt sein Vorgehen mit dem Mitwir-

kungsgrundsatz nach § 26 Abs. 2 Satz 1 ThürVwVfG begründete, erfüllt diese Rechtsvorschrift nach Ansicht des TLfDI nicht die Voraussetzungen des Art. 14 Abs. 5 Buchstabe c) DS-GVO. Es bedarf daher auch hier der Information der betroffenen Person nach der DS-GVO.
Auch führt die Übermittlung der Schuldnerdaten von Dritten (§ 74a SGB X oder das Gesetz zu Verbesserung der Sachaufklärung in der Verwaltungsvollstreckung) nach den obigen Ausführungen nicht zum Verzicht auf die Informationspflichten nach der DS-GVO. Ebenfalls bedarf es in diesen Fällen einer Information der betroffenen Personen. Die Vollstreckungsbehörde als Empfänger der übermittelnden Daten erhebt diese übermittelten Daten und ist darum grundsätzlich verpflichtet, der betroffenen Person die Informationen mitzuteilen.
Abschließend hat der TLfDI das Landratsamt noch darauf hingewiesen, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gemäß § 32h AO für die Aufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der AO zuständig ist.

3.20 Datensicherheit beim Telefax

Im Gegensatz zur Briefpost handelt es sich bei einem Telefax um eine Art „offene Zustellung“. Deshalb müssen bei einem Versand von personenbezogenen Daten per Fax Maßnahmen getroffen werden, die verhindern, dass bei der Übertragung diese Daten unbefugt gelesen, verändert oder gelöscht werden können.

Eine Bürgerin beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über einen Arbeitgeberverband, der das Sitzungsprotokoll der arbeitsrechtlichen Streitigkeit zwischen der Bürgerin und dem Arbeitgeber der Bürgerin (einem Verbandsmitglied des Arbeitgeberverbandes) per Telefax an dritte Personen übermittelte. Der Arbeitgeberverband vertritt die Gesamtheit seiner Mitglieder, mithin auch den Arbeitgeber der Bürgerin, zum Beispiel gegenüber der Gewerkschaft, der Politik, gegenüber Architekten- und Ingenieurverbänden und auch gegenüber öffentlichen Auftraggebern. Darüber hinaus haben die Verbandsmitglieder und damit der Arbeitgeber auch Anspruch auf kostenlose Vertretung bei Arbeits- und Sozialgerichtsverfahren bis in die zweite Instanz. Hier vertrat der Arbeitgeberverband sein Mitglied, den Arbeitgeber der Bürgerin, in deren arbeitsrechtlicher Streitigkeit.

Der TLfDI wandte sich daraufhin an den Arbeitgeberverband und bat um Stellungnahme zu den geschilderten Vorwürfen.
Dieser führte aus, dass er auf Wunsch des Arbeitgebers und Verbandsmitglieds das Sitzungsprotokoll der privatrechtlichen Streitigkeit der Bürgerin an das zentrale Fax gesendet habe. Im Adressfeld des Schreibens sei durch den Arbeitgeberverband klar erkennbar das Personalamt des Verbandsmitglieds und Arbeitgebers der Bürgerin benannt worden. Die Beschäftigten der Poststelle des Verbandsmitglieds haben daraufhin versehentlich das Fax an die Bürgerin direkt, wegen ihres fett hervorgehobenen Namens im Betreff, als elektronisches Fax weitergeleitet. Auf dieses Postfach der Bürgerin, in dem die elektronischen Faxe eingehen, haben auch unbeteiligte Dritte aufgrund von Vertretungsregelungen Zugriff. So erfolgte es auch in diesem Fall. Daraufhin sei unmittelbar nach Bekanntwerden der Fehlleitung das Dokument gelöscht und der Vorfall mit der Beschäftigten der Poststelle ausgewertet worden. Daraufhin habe der Arbeitgeber die Beschäftigten der Poststelle auf ordnungsgemäße, dem jeweiligen Adressaten entsprechende Verteilung der Faxe als auch sämtlicher Post hingewiesen.
Diese Verfahrensweise sah der TLfDI als erforderliches und wirksames Mittel an, um künftiges Fehlverhalten der geschilderten Art von vornherein ausschließen beziehungsweise beseitigen zu können. Im Gegensatz zur Briefpost handelt es sich bei einem Telefax um eine Art offene Zustellung. Deshalb müssen bei einem Versand von personenbezogenen Daten per Fax Maßnahmen getroffen werden, die verhindern, dass bei der Übertragung diese Daten unbefugt gelesen, verändert oder gelöscht werden können.
Darüber hinaus hat der TLfDI sowohl den Verband als auch das Mitglied darauf hingewiesen, dass Faxgeräte (elektronisch oder manuell), die von mehreren Mitarbeitern einer öffentlichen Stelle genutzt werden können, zukünftig nicht mehr als Empfangsgeräte genutzt werden sollten. Der Verband bestätigte dem TLfDI, dass er Protokolle oder Ähnliches grundsätzlich nicht per Fax versende. Dies erfolge nur auf Wunsch der Mitglieder oder nach Rücksprache mit dem Mitglied, wenn gerichtlich gesetzte Fristen andernfalls – aufgrund der mittlerweile unnormal längerdauernden Postlaufzeiten – nicht eingehalten werden könnten. Auch das Mitglied stimmte den Hinweisen des TLfDI zu.

Weitere Maßnahmen des TLfDI nach Art. 58 Abs. 2 Datenschutz-Grundverordnung in Verbindung mit § 7 Abs. 1 Thüringer Datenschutzgesetz waren nicht zu treffen.

3.21 Was darf in Dienstplänen mitgeteilt werden?

Es gibt keine Rechtsgrundlage dafür, in für andere Mitarbeiter zugänglichen Kalendern, Plänen und Listen Informationen zu Fehltagen aufgrund von Erkrankung oder Erkrankung des Kindes einzutragen. § 27 Thüringer Datenschutzgesetz in Verbindung mit den dienstrechtlichen Vorschriften erlaubt es nur, eine Abwesenheit der Beschäftigten darzustellen, soweit deren Kenntnis für die Kollegen erforderlich ist. Eine Nennung des Grundes für die Abwesenheit ist keinesfalls erforderlich.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum nicht nur aus Unternehmen, sondern auch aus öffentlichen Stellen Anfragen zur Zulässigkeit von für alle Beschäftigten einsehbaren Kalendern, Zeitplänen oder Tabellen, in denen aufgeführt ist, wer wann aus Gründen der Erkrankung (des Mitarbeiters selbst oder eines Kindes) der Arbeit fernblieb. Besonders interessant für andere Beschäftigte wird es dann, wenn man die angefallenen Krankheitstage aufsummieren und vergleichen kann.
Aufgrund der Öffnungsklausel Art. 88 Datenschutz-Grundverordnung hat das Land Thüringen von der Möglichkeit Gebrauch gemacht und mit § 27 Thüringer Datenschutzgesetz (ThürDSG) spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten geschaffen. § 27 Abs. 1 Thür DSG wiederum erklärt die dienstrechtlichen Vorschriften §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) für entsprechend anwendbar, soweit besondere Rechtsvorschriften des Arbeitsrechts, tarifvertragliche Regelungen oder Dienstvereinbarungen nichts Abweichendes regeln. Soweit es für den Dienstherrn erforderlich ist, die Abwesenheitsgründe zu verarbeiten, ist die Führung einer An- und Abwesenheitsliste der Beschäftigten auf der Grundlage des § 27 ThürDSG sowie der dienstrechtlichen Vorschriften §§ 79 bis 87 ThürBG möglich. Keine Rechtsgrundlage besteht mangels Erforderlichkeit allerdings dafür, die Angaben in der Liste zu privat oder persönlich bedingten Abwesenheiten (Krankheit,

Kind krank, Urlaub etc.) den anderen Beschäftigten zur Kenntnis zu geben. Anderen Beschäftigten darf allenfalls, sofern eine Erforderlichkeit begründet werden kann, zur Kenntnis gegeben werden, ob ein Mitarbeiter ansprechbar ist oder sich nicht im Dienst befindet. Hierzu reicht es aus, die betreffenden Mitarbeiter als „abwesend“ zu kennzeichnen. Die Gründe der Abwesenheit sind nicht relevant und daher auch nicht zur Einsicht bereitzustellen. Lediglich im Falle einer dienstlich bedingten Abwesenheit, zum Beispiel wegen Dienstreise, bestünden keine Bedenken gegen eine Kenntnisnahmemöglichkeit, da es sich um ein dienstliches Datum handelt.
Für die Kenntnisnahme der insgesamt für einen Kollegen angefallenen Krankheitstage für alle Beschäftigten gibt es ebenfalls keine Rechtsgrundlage. Es ist daher unzulässig, den anderen Mitarbeitern die Abwesenheitsgründe und die Krankheitstage in der Summe zur Kenntnis bereitzustellen.

3.22 Weitergabe von Fehlzeiten und Noten durch die Berufsschule jetzt geregelt

Während der TLfDI bisher die Ausbildungsbetriebe auf die Unzulässigkeit von Anfragen bei der Berufsschule nach Fehlzeiten und Notenständen ihrer Auszubildenden hingewiesen hat, wurden die berufsbildenden Schulen mit der Anfügung eines § 47 Abs. 9 Thüringer Allgemeine Schulordnung nunmehr gesetzlich dazu verpflichtet, die Ausbildungsbetriebe über diese Sachverhalte zu unterrichten.

Eine Rechtsanwaltskanzlei wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob die von ihr vertretene Arztpraxis die Noten und Fehlzeiten einer dort beschäftigten Auszubildenden bei der zuständigen Berufsschule abfragen darf oder ob die Arztpraxis hierzu zuvor eine rechtswirksame Einwilligung, die von der Berufsschule erstellt wurde, bei der Auszubildenden einzuholen hat. Die Kanzlei hielt es für zwingend erforderlich, anhand der Fehlzeiten der Auszubildenden zu erfahren, ob diese die Berufsschule regelmäßig besucht hat, da der Arbeitgeber ansonsten keine Kontrollmöglichkeiten habe.
Der TLfDI teilte der Kanzlei in seiner Stellungnahme mit, dass der Ausbilder ein berechtigtes beziehungsweise sogar ein rechtliches Interesse an der Kenntnis von unentschuldigten Fehlzeiten hat. Da zum Zeitpunkt der Anfrage aber keine gesetzliche Befugnis vorlag, die es

der Berufsschule erlaubt hätte, die Fehlzeiten oder die aktuellen Noten der Schülerin an den Ausbildungsbetrieb zu übermitteln, musste sich dieser die erforderlichen Informationen ausschließlich bei seiner Auszubildenden beschaffen. Bei begründeten Zweifeln an diesen Angaben sah es der TLfDI als zulässig an, sich von der Auszubildenden eine schriftliche Bestätigung der Berufsschule über die An- und Abwesenheiten vorlegen zu lassen. Die von den Industrie- und Handelskammern entworfene Einwilligungserklärung, in der Auszubildende sich mit der Übermittlung ihrer Fehlzeiten und Noten einverstanden erklären sollten, wurde vom TLfDI sehr kritisch gesehen. Der Auszubildende steht in einem Über- / Unterordnungsverhältnis sowohl mit dem Ausbildungsbetrieb als auch mit der Berufsschule als staatliche Stelle. Eine Einwilligung, die auf der freien Entscheidung des Auszubildenden beruht, war somit nicht möglich. Für einen Ausbildungsbetrieb gilt gemäß § 26 Abs. 2 Bundesdatenschutzgesetz eine ausdrückliche Regelung im Beschäftigtenbereich, wonach Beschäftigte nur dann freiwillig in eine Verarbeitung ihrer Daten einwilligen können, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen (siehe hierzu Kurzpapier Nr. 14 der Datenschutzkonferenz unter: https://www.tlfdi.de/mam/tlfdi/themen/dsk_nr14_beschaftigtendatenschutz.pdf).

Nachdem der TLfDI sich mit der Problematik und Eingaben von Ausbildungsbetrieben, Berufsschullehrkräften und Auszubildenden hierzu fast zwei Jahre lang beschäftigt hat, gibt es seit dem 31. Oktober 2019 mit der Einfügung eines § 47 Abs. 9 Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen eine Rechtsgrundlage, die die Berufsschulen verpflichtet, die Auszubildenden über unentschuldigte Fehlzeiten, verhängte Ordnungsmaßnahmen und einen deutlichen Abfall der schulischen Leistung zu informieren. Der Ausbildungsbetrieb hat darüber hinaus einen Anspruch, Auskunft über den Leistungsstand seines Auszubildenden bei der Schule einzuholen. Anfragen wie die oben genannte dürften sich damit zukünftig erledigt haben.

3.23 Mitarbeiterüberwachung: Gleiches mit Gleichem vergelten?

Muss zur Überprüfung von Unregelmäßigkeiten auf Mitarbeiterrechner zugegriffen werden, sind die diesbezüglichen Festlegungen zu beachten. Vermuten oder befürchten Mitarbeiter unberechtigte Zugriffe auf ihre Arbeitsplatzrechner, sind sie dennoch nicht befugt, den Spieß umzudrehen und ihrerseits den Dienstvorgesetzten zu überwachen. Nicht alle Systeme, die eine Auslastungsfeststellung ermöglichen, ermöglichen auch eine Leistungs- und Verhaltenskontrolle.

Der vorliegende Fall gestaltete sich recht komplex und der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde erst einmal auf eine falsche Fährte geführt: Der TLfDI erhielt zunächst einen anonymen Hinweis, dass bei einer öffentlichen Stelle (Verantwortlicher) Software zum Einsatz komme, die die Mitarbeiterüberwachung ermögliche. Um welche Software es sich handelte, wurde nicht mitgeteilt. Aus der Schilderung, dass die angemeldeten Nutzer hinsichtlich der geöffneten Dokumente, Tastenanschläge, verwendeter Software, aufgerufener Webseiten und privater Daten innerhalb von Domainaccounts überwachbar seien und einzelne erhobene Datensätze zusammengeführt werden können, sah dies nach einer Leistungs- und Verhaltenskontrolle von Beschäftigten aus. Der TLfDI fragte daher beim Verantwortlichen nach, was es damit auf sich habe und ob man derartige Mitarbeiterüberwachung betreibe.
Der Verantwortliche führte aus, die Dienstvereinbarung zur Einführung und Anwendung von IT-Systemen schließe die missbräuchliche Nutzung von IT-Systemen zur Leistungs- und Verhaltenskontrolle aus. Im IT-Bereich setze man grundsätzlich auch keine Software ein, die die Leistung und das Verhalten von Mitarbeitern überwache. Für die Analyse von Systemressourcen und die Unterstützung des Helpdesks seien allerdings notwendige Softwaretools etabliert, die insbesondere dazu dienten, den ordnungsgemäßen Zustand und reibungslosen Betrieb der einzelnen IT-Systeme zu gewährleisten. Im Übrigen bereite man eine ISO-Zertifizierung vor, welche auch ein Ressourcenmanagement beinhalte.
Das aus diesem Grund angeschaffte Clientanalysetool zur Analyse der Systemressourcen habe man vor dessen Einführung dem Personalrat vorgestellt, die Zustimmung zur Einführung liege vor.
Weiterhin betreibe und verwalte man ein sogenanntes Assetmanagement, das zur Inventur der eingesetzten Hard- und Software notwen-

dig sei, was dem Personalrat ebenfalls bekannt sei. Dieses Assetmanagement-System solle zur schnellen Erkennbarkeit von Angriffen auf die IT-Sicherheit und zur rückwirkenden Fehlerrecherche genutzt werden. Dazu werden sowohl globale Alarme bei Detektion eines Angriffs, als auch Detailinformationen zu einem bestimmten Rechner angezeigt. Diese Informationen betreffen Netzwerkverbindungen, die CPU-Statistik und Informationen zu Anwendungen. Durch die entsprechende Angabe der Rechner kann auf die Nutzer zurückgeschlossen werden. Insoweit ist auch eine Personenbeziehbarkeit gegeben. Durch eine Dienstanweisung wurde eine Leistungskontrolle organisatorisch verhindert. Hierzu gab der TLfDI den Hinweis, dass man bestimmte Daten auch unterdrücken könne, womit eine Leistungskontrolle ebenfalls ausgeschlossen werden könnte.
Nach kursorischer Prüfung dieser Faktenlage gelangte der TLfDI zunächst zu der Auffassung, dass die vom Verantwortlichen geschilderten Gegebenheiten nicht mit den anonym geschilderten Überwachungsmöglichkeiten in Einklang gebracht werden konnten, denn einen Zugriff auf Inhalte ermöglichten die eingesetzten Tools nicht. Vielmehr erschienen die geschilderten getroffenen organisatorischen Maßnahmen grundsätzlich erforderlich und geeignet, den Grundsätzen für die Verarbeitung personenbezogener Daten nach Art. 5 der Datenschutz-Grundverordnung (DS-GVO) und dem Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen nach Art. 25 DS-GVO Rechnung zu tragen.
Nachdem die Untersuchungen beim TLfDI bereits liefen, wandte sich nun auch der Personalrat des Verantwortlichen an den TLfDI und bat um die Überprüfung eines Falles, bei dem ein Dienstvorgesetzter mutmaßlich unberechtigt auf personalisierte Mitarbeiter-PCs zugegriffen hatte und die Dienststelle dies lediglich als einen Verstoß gegen Compliance-Richtlinien bewertet hatte, nicht aber als Verstoß gegen Datenschutzbestimmungen. Dieser Sachverhalt betraf nicht die bereits geprüften Tools zum Assetmanagement und zur Unterstützung des Helpdesks, sondern beschrieb vielmehr einen Vorfall, bei dem möglicherweise Nutzer mit Administratorrechten gegeneinander arbeiteten. Kurz darauf bat auch der Verantwortliche den TLfDI, ihn bei der Aufarbeitung des Sachverhalts zu beraten, der intern bereits umfangreichen Überprüfungen unterzogen worden war. Dieser Sachverhalt passte nun auch besser zur anonymen Beschwerde.
Im Rahmen des Gesprächs vor Ort mit Vertretern des Verantwortlichen und des Personalrats konnte Folgendes weiter geklärt und im An-

schluss datenschutzrechtlich bewertet werden: Demnach hatte der Dienstvorgesetzte auf den dienstlichen Rechner eines Administrators zugegriffen, weil die Softwareverteilung bei einigen PCs nicht funktioniert hatte und er feststellen wollte, ob ein technisches Problem vorlag. Tatsächlich war für die Administratoren eine nicht genehmigte Ausnahmengruppe gebildet worden, sodass die Software auf die zu dieser Gruppe gehörenden PCs nicht eingespielt werden konnte. Bei dieser Gelegenheit wollte der Dienstvorgesetzte auch gleich überprüfen, ob eine bekannt gewordene ominöse Software mit der Bezeichnung „Lauschangriff“ auch auf diesem PC existierte. Hierzu war der Dienstvorgesetzte nach den internen Feststellungen befugt, denn damit lagen Hinweise auf die Gefährdung der IT-Sicherheit vor, die sich allerdings nicht bestätigten.
Im Zuge der Überprüfung wurde aber auch festgestellt, dass auf den Arbeitsplatzrechnern der Mitarbeiter des Helpdesks eine Software mit der beschreibenden Bezeichnung „Don’t spy me“ installiert war, womit Zugriffe des Dienstvorgesetzten dokumentiert werden konnten. Für eine derartige Vorgehensweise durch die Mitarbeiter gab es keine Berechtigung. Die durch diese Software gewonnenen Logdaten sollten nun gegen den Vorgesetzten eingesetzt werden und ihn der Spionage überführen.
In diesem Zusammenhang kam der TLfDI zu folgendem Schluss: Zum einen hätte der Einsatz der „Don’t spy me“-Software genehmigt werden müssen, zum anderen hätte der Dienstvorgesetzte für die weitergehenden Recherchen allerdings nach den Festlegungen im Falle von Verstößen den IT-Sicherheitsbeauftragten und/oder den Datenschutzbeauftragten der Stelle hinzuziehen müssen, damit dem „Vier-Augen-Prinzip“ Rechnung getragen ist. Mit dieser Feststellung wurde ein Teilproblem der Beschwerde gelöst.
Ob der Dienstvorgesetzte allerdings tatsächlich auf Inhalte von Dateien zugegriffen hatte, ließ sich im Nachhinein nicht mehr mit Sicherheit aus den Logfiles rekonstruieren. Die Logdatei zeigte zwar Zugriffe auf den lokalen Rechner, wobei erkennbar war, dass Verzeichnisse systematisch durchsucht wurden, nicht jedoch, ob durch den Vorgesetzten auch lesend auf Inhalte Zugriff genommen wurde.
Zu der eingangs beschriebenen anonymen Beschwerde stellte sich weiterhin heraus, dass offenbar ein Telefonserversystem gemeint war, mittels dessen ein Supervisor in einer Momentaufnahme feststellen kann, welche namentlich benannten Personen gerade angemeldet sind und wer kein Gespräch führt. Außerdem ermöglicht das System eine

Statistik, wie viele Anrufe erfolgten und angenommen wurden, wobei die Auslastung für den gesamten Pool dargestellt wird. Es ermöglicht jedoch nicht, einzelne Apparate zu überwachen und ist daher nicht geeignet, einzelne Mitarbeiter einer Leistungs- und Verhaltenskontrolle zu unterziehen.
In Aufarbeitung der Angelegenheit hatte der Verantwortliche bereits einen Maßnahmenkatalog vorbereitet. Die darin vorgeschlagenen und teilweise bereits umgesetzten Maßnahmen betrachtete der TLfDI in der Summe als geeignet, angemessen und ausreichend, um die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen.

3.24 Beihilfe: Digitalisierung des Antragsverfahrens

Durch die Digitalisierung in Antragsverfahren können Kosten, Zeit und Aufwand für den Bürger und die Verwaltung verringert werden. Bevor aber Anträge und beizufügende Unterlagen digital übermittelt werden können, bedarf es hinsichtlich der Vereinbarkeit mit datenschutzrechtlichen Vorschriften der genauen Prüfung, insbesondere, wenn es um sensible personenbezogene Daten geht.

Bislang müssen die Beihilfeberechtigten einen Vordruck ausfüllen und in Papierform unter Beifügung von Kopien der Rechnungen für ärztliche Leistungen, Heilmittel, Rezepte für Medikamente etc.der Beihilfestelle übersenden. Das Thüringer Finanzministerium (TFM) als das für die Beihilfe zuständige Ressort, wandte sich im Jahr 2018 an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da beabsichtigt sei, bis Mitte 2019 die Beantragung von Beihilfeleistungen sowohl für aktive Beamte als auch für Versorgungsbezügeempfänger über das Thüringer Antragssystem für Verwaltungsleistungen (ThAVEL) elektronisch zu ermöglichen. Da hierbei sensible, insbesondere Gesundheitsdaten der Antragsteller verarbeitet werden, bat das TFM frühzeitig um eine Verständigung mit dem TLfDI hinsichtlich der inhaltlichen und technischen Voraussetzungen, um den datenschutzrechtlichen Vorgaben Rechnung zu tragen.
Vom TFM war zunächst angedacht, allen Beschäftigten der einzelnen Ressorts die Möglichkeit einzuräumen, ihre Beihilfeanträge auszufüllen und Anlagen (Rechnungen und Rezepte mit Diagnoseangaben zu Abrechnungszwecken) auch über einen dienstlichen Rechner hochladen und an die Beihilfestelle senden zu können. Der TLfDI wies da-

rauf hin, es müsse sichergestellt sein, dass die jeweilige Beschäftigungsdienststelle auf keine gespeicherten oder eingescannten Dokumente und damit auf darin gegebenenfalls enthaltene Diagnosen und Rezepte Zugriff nehmen kann. Es sollte daher auf keinen Fall eine Speicherung auf dem PC oder Server der Dienststelle erfolgen.
Das TFM teilte daraufhin dem TLfDI mit, die ursprünglich in Erwägung gezogene Eröffnung der Möglichkeit, die Beantragung über Dienst-PC auch unter Nutzung von dienstlicher Hardware (Scanner) zu ermöglichen, werde vorerst nicht weiterverfolgt.
Weiterhin teilte das TFM mit, dass an der Erstellung eines IT-Sicherheitskonzeptes und der Datenschutz-Folgenabschätzung nach Art. 35 Datenschutz-Grundverordnung gearbeitet werde und das Ministerium, sobald die Datenschutz-Folgenabschätzung im Entwurf vorliegt, wieder auf den TLfDI zukomme. Der TLfDI wird über das weitere Verfahren berichten.

3.25 DigitalPakt: Digitalstrategie des Thüringer Bildungsministeriums – Datenschutz ist mit im Boot

Für die Umsetzung des DigitalPakts von Bund und Ländern unter Thüringer Schuldächern hat das TMBJS eine „Digitalstrategie Thüringer Schule“ entwickelt. Der TLfDI unterstützt dabei sowohl beim Bildungsmanagement als auch bei der Medienbildung.

Schulen sind abgehängt vom Schnellzug in das Digitalzeitalter – so oder ähnlich klingt’s, wenn man in manche Thüringer Schule hineinhört: Computerräume mit dem Charme der Jahrtausendwende, eine schwache DSL-Leitung ins Schulhaus, kein WLAN und Lehrer, die mit ihrem privaten Laptop anrücken. Nein, es gibt auch andere Beispiele: iPad-Klassen, Whiteboards, die auch tatsächlich genutzt werden, Grundschüler, die mit dem Calliope programmieren lernen. Die Unterschiede sind groß, und das nicht nur in Thüringen. Dass das nicht so bleiben kann, haben Bundes- und Landespolitiker erkannt und den „DigitalPakt Schule 2019 bis 2024“ auf den Weg gebracht, der 5 Milliarden Euro Förderung vom Bund für die Schulen im gesamten Bundesgebiet vorsieht. Die Länder legen nochmal 10 % drauf. Mit dem ordentlichen Brocken kann viel passieren für und in den Schulen.
Das Thüringer Bildungsministerium ist verantwortlich, was *in* den Schulen passiert, hat landesspezifische Schwerpunkte gesetzt und in der „Digitalstrategie Thüringer Schule (DiTS)“ verankert. Hier geht

es nicht um Glasfaseranschlüsse für Schulen, sondern um Inhalte für veränderten Unterricht, um Professionalisierung von Lehrkräften und ein zeitgemäßes Bildungsmanagement, zum Beispiel durch eine Landeslösung für die Kommunikation von Lehrkräften und einer Thüringer Schul-Cloud. Gerade dabei ist klar, dass viele Daten ausgetauscht werden, die in schulischem Kontext fast immer personenbezogen sind. Klar ist auch, dass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einen Fuß in der Tür haben muss. Schließlich sollen die Daten der Schüler, Eltern und Lehrkräfte nicht auf Abwege geraten. Das Bildungsministerium sieht das ebenso und hat das Unterstützungsangebot des TLfDI aufgegriffen. So wirkt der der TLfDI an der Bereitstellung eines E-Mail-Systems für alle staatlichen Lehrkräfte (siehe Beitrag Nummer 3.29) sowie einer landesweiten Lernplattform mit. Spannend bleibt, wie die wiederholten Unterstützungsimpulse des TLfDI aufgegriffen werden, wenn es um konkrete Inhalte des neuen Unterrichtsfachs „Informatik und Medienbildung“ gehen wird, das es zukünftig ab Klassenstufe 5 geben soll. Gerade hier wäre Platz, Schülerinnen und Schüler für den Schutz der Privatsphäre zu sensibilisieren und Kompetenzen für praktischen Selbstdatenschutz zu entwickeln. Und last but not least: Wie werden Pädagogen dafür fit gemacht? Der TLfDI wird auch weiterhin nicht lockerlassen, wenn es um eine angemessene Platzierung von Datenschutzfragen in allen drei Phasen der Lehrerbildung geht.

3.26 Die Schul-Cloud des Hasso-Plattner-Instituts steht in abgespeckter Form vor Einführung in Thüringer Pilotschulen

Die vom Hasso-Plattner-Institut (HPI) entwickelte und bundesweit angebotene Schul-Cloud wird in einer abgespeckten Form als „Thüringer Schul-Cloud“ zunächst in 20 Pilotschulen und fünf Gymnasien in staatlicher Trägerschaft erprobt werden. Die seit Langem kritische Begleitung der HPI-Schul-Cloud durch den TLfDI erstreckt sich nunmehr auch auf die „Thüringer Schul-Cloud“.

Grob skizziert, handelt es sich bei der Schul-Cloud des Hasso-Plattner-Instituts (HPI) um eine Lernplattform, wie sie von vielen Marktteilnehmern derzeit für den Schulbereich in ähnlicher Form angeboten wird. Die Plattform beruht auf einer Cloud-Lösung, das heißt, es findet eine zentrale Datenhaltung statt, worauf nach der Vergabe von definierten Zugriffsrechten über ein Login-Verfahren zugegriffen wer-

den kann. Die Schul-Cloud dient zum einen der Kommunikation, beispielsweise innerhalb einer Klasse zwischen den Schülerinnen und Schülern und den Lehrkräften, und zum anderen der Bereitstellung von Lerninhalten. Die Lehrkräfte können beliebige Informationen, etwa Hausaufgaben, Arbeitsblätter, Formeln, Vokabeln und so weiter für die Klasse in die Cloud einstellen, die dann zeit- und ortsunabhängig von den Schülerinnen und Schülern abgerufen und auch bearbeitet werden können. Darüber hinaus erlaubt die HPI-Schul-Cloud über Schnittstellen das Integrieren von verschiedenen externen Diensten, auf die dann ebenfalls ein Zugriff von den Nutzern möglich wird. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte sich bereits in seinem 12. Tätigkeitsbericht unter Nummer 16.5 kritisch mit den Cloud-Lösungen für Schulen beschäftigt.

Lange Zeit bevor überhaupt feststand, dass auch Thüringen eine Schul-Cloud auf der Basis der Schul-Cloud des Hasso-Plattner-Instituts (HPI-Schul-Cloud) einführen wird, beschäftigte sich der TLfDI in seiner Eigenschaft als Vorsitzender zweier Arbeitskreise „Schulen und Bildungseinrichtungen“ sowie „Datenschutz- / Medienkompetenz“ mit der HPI-Schul-Cloud. Bereits im Jahre 2017 verkündete der TLfDI bei seiner ersten Einladung zu einer HPI-Schul-Cloud-Sitzung, dass der Datenschutz zu beachten ist und „rote Linien“ beschrieben werden müssen, die unbedingt einzuhalten sind. Als dann dem TLfDI bekannt wurde, dass das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) für zunächst 20 Thüringer Pilotschulen, fünf Spezialgymnasien in staatlicher Trägerschaft sowie 17 Einrichtungen der Thüringer Lehrerausbildung eine „Thüringer Schul-Cloud“ einführen wird, die auf der HPI-Schul-Cloud beruht, wandte sich dieser an das Ministerium, um über die bestehenden datenschutzrechtlichen Bedenken bei der Nutzung der HPI-Schul-Cloud zu informieren. Dies betraf bisher insbesondere den Inhalt der inzwischen fast 300 Seiten langen Dokumente: das Sicherheitskonzept, die Datenschutz-Folgenabschätzung, die Einwilligungserklärung, den Auftragsverarbeitungsvertrag und vieles mehr. Bisher hat das HPI die vom TLfDI geäußerte Kritik stets aufgenommen und Änderungen an den Papieren vorgenommen. Die datenschutzrechtliche Bewertung der reinen HPI-Schul-Cloud ist als weitgehend abgeschlossen anzusehen. Nach Auffassung des TLfDI liegt ein großes Problem der HPI-Schul-Cloud bei den oben erwähnten Schnittstellen, die die Cloud bietet. Über diese Schnittstellen können die Nutzer auf zahlreiche Anbieter im Internet zugreifen,

die Lehr- und Lerninhalte für die Schülerinnen und Schüler anbieten. Bei der datenschutzrechtlichen Kontrolle einer Schule in Thüringen, die die HPI-Schul-Cloud in der vom HPI bereits seit längerer Zeit angebotenen Form bundesweit anbietet, hatte sich der TLfDI einen Schüler-Test-Account anlegen lassen und die Funktionen der Schul-Cloud geprüft. Dabei wird über einen sogenannten Lern-Store auf verschiedene Inhalte-Anbieter zugegriffen und deren Webangebot analysiert. Die Klardaten der Nutzer (Schülerinnen und Schüler) werden in der Schul-Cloud pseudonymisiert, sodass die Inhalte-Anbieter nur Pseudonyme erhalten. Allerdings sind auch pseudonymisierte Daten zumindest dann personenbezogen, wenn beim Inhalteanbieter durch den Kontakt mit dem pseudonymisierten Nutzer weitere Daten anfallen, etwa, wenn Freitextstellen in einem Übungsbogen ausgefüllt werden, die IP-Adresse des Nutzers dem Inhalte-Anbieter bekannt wird und Ähnliches. Hierbei besteht die Gefahr, dass das Datenverarbeitungsgerät (und damit der Nutzer) ohne Umweg über die HPI-Schul-Cloud direkt vom Inhalte-Anbieter, etwa aus Werbegründen, kontaktiert wird. Eine Profilbildung wäre dann zumindest möglich. Die Analyse ergab weiterhin, dass diese Anbieter mehrere Analysetools einsetzen, etwa Google Analytics. Auch Verknüpfungen, die die Nutzer tracken, also verfolgen können, bestehen, etwa mit Facebook. Die ungefilterte Nutzung des Internets über die HPI-Schul-Cloud sieht der TLfDI derzeit als das Hauptproblem an. Hier wird durch die von der Schule bereitgestellte Schul-Cloud während des Unterrichts die Domäne des HPI verlassen und es werden über eine Weiterleitung auf Drittseiten Inhalte angeboten, welche zumindest datenschutzrechtlich bedenklich sind. Es wird einzig der Hinweis gegeben: „Sie verlassen jetzt die Schul-Cloud. Sie werden auf die Seite von … weitergeleitet“. Nur wenige Inhalte konnten beim Testzugriff als datenschutzgerecht in der Schul-Cloud eingebunden bezeichnet werden. Das HPI teilte dem TLfDI zur Problematik mit, dass die Bereitstellung der jeweiligen Inhalte-Anbieter in den Verantwortungsbereich der Schule fiele, entsprechende Zugriffe müssten dann gesperrt werden.
Das TMBJS ließ wissen, dass die „Thüringer Schul-Cloud“ über das Thüringer Schulportal zur Verfügung gestellt werden soll. Das Thüringer Schulportal ist eine Arbeitsplattform, die Informationen, Materialien und Serviceleistungen für den Thüringer Bildungsbereich zur Verfügung stellt. Wie sich gezeigt hat, entfallen zwar die oben beschriebenen Schnittstellen zu ungeprüften Inhalte-Anbietern, leider sind aber auch in das Thüringer Schulportal Inhalte-Anbieter einge-

bunden, gegen welche datenschutzrechtliche Bedenken bestehen. So ist beispielsweise die Lernplattform „serlo.org“ eingebunden. Dort sind mehrere Trackerdienste aktiv. Dies betrifft insbesondere Google Analytics, da die dort angegebenen Daten in die USA übermittelt werden. Wer die Datenschutzerklärung liest, erfährt zwar, dass man die Erfassung durch Google Analytics verhindern kann, dies betrifft aber frühestens die Folgebesuche der Seite. Außerdem wird mit Hotjar ein weiterer Webanalysedienst eingesetzt, der zwar im Geltungsbereich der Datenschutz-Grundverordnung (DS-GVO) seinen Sitz hat, jedoch auch erst nach dem ersten Besuch der Seite deaktiviert werden kann. Weitere Datenübertragungen erfolgen mit den Tools Vimeo, Google-Web Fonts, die Google Cloud sowie Google reCAPTCHA.
Die Nutzung von Trackern darf aus Sicht des TLfDI nur nach der Erklärung einer Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO erfolgen. Daher darf in dieser Konstellation serlo.org mit diesen Diensten in Thüringer Schulen den Schülerinnen und Schülern über die Schul-Cloud nicht angeboten werden. Der TLfDI ist bisher über die Einführung und den Betrieb der „Thüringer Schul-Cloud“ nur sehr unvollständig unterrichtet. Insbesondere liegen die erforderlichen schriftlichen Unterlagen, die vor der Einführung des Verfahrens erstellt werden müssen, noch nicht vor. Der TLfDI wird seine datenschutzrechtliche Prüfung fortsetzen und dabei auch bei einer Pilotschule eine Vor-Ort-Kontrolle durchführen.

3.27 Liveübertragung des Unterrichts aus dem Klassenzimmer?

Schulpflichtigen Kindern, denen es nicht möglich ist, über längeren Zeitraum oder sogar dauerhaft an dem Unterricht ihrer Schule teilzunehmen, sollte die Möglichkeit geboten werden, sich grundlegende Bildungsinhalte aneignen zu können. Digitale Lernkonzepte wie beispielsweise ein Einsatz von Telepräsenzavataren in den Klassenräumen könnten einer der vielen Lösungswege sein, wenn von allen Beteiligten die schriftliche Einwilligung vorliegt.

Im Januar 2019 wandten sich Eltern, deren Kind aufgrund einer Erkrankung über einen längeren Zeitraum nicht am regulären Unterricht der Schule teilnehmen konnte, an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie favorisierten eine Lösung in Form von Liveübertragung des Unterrichts und baten den TLfDI, dies aus datenschutzrechtlicher Sicht zu prüfen.

Zurzeit besteht die Regelung, dass Schulpflichtige, die sich sechs Wochen und länger oder wiederholt in medizinischen Einrichtungen aufhalten und deshalb nicht am Unterricht der Schule teilnehmen können, Grundlagenunterricht erhalten sollen, so § 54 Abs. 1 Thüringer Schulgesetz (ThürSchulG). Befinden sich die Schulpflichtigen in häuslicher Pflege, können sie Hausunterricht in den Grundlagenfächern gemäß § 54 Abs. 2 ThürSchulG erhalten. Der Hausunterricht wird allerdings in einer Kann-Bestimmung geregelt, und somit hat der Schüler keinen unmittelbaren Anspruch darauf, sondern lediglich einen Anspruch auf ermessenfreie Entscheidung. Sollte der Unterricht erteilt werden, erfolgt dieser nur in den Grundlagenfächern. So könnten betroffene Kinder mit minimaler Beschulung womöglich nie einen Abschluss erreichen.
Die Recherchen des TLfDI ergaben, dass es technisch mehrere Möglichkeiten der Liveübertragung von Schulunterricht gibt, so etwa den Einsatz von Telepräsenzavataren in Klassenräumen. Es gibt beispielsweise einen Roboter, welcher auf den Tisch des fehlenden Schülers zu stellen wäre. Dieser kann den Unterricht live auf das Endgerät des erkrankten Schülers übertragen. Der Avatar ist mit einer Kamera, einem Lautsprecher und einem Mikrofon ausgestattet. Ebenso kann er um 360 Grad gedreht werden und es besteht die Möglichkeit, durch LED-Lichter vorprogrammierte Emotionen sowie das Melden oder das passive Teilnehmen des Kindes am Unterricht zum Ausdruck zu bringen.
Der TLfDI stand vor der Aufgabe, die technisch mögliche Liveübertragung auf datenschutzrechtliche Aspekte zu prüfen, damit Beeinträchtigungen der Rechte der betroffenen Personen ausgeschlossen werden können. Bei einer Liveübertragung werden unter Umständen Bilder vom Unterricht und personenbezogene Daten der Lehrkraft und der anderen Schüler, die sich jeweils im Bild befinden, übertragen. Zudem wäre eine Speicherung der Liveübertragung nicht ausgeschlossen. Nach den ersten Einschätzungen wäre eine Liveübertragung des Unterrichts daher nur möglich, wenn alle Beteiligten, also die Lehrer, alle Eltern und Schüler der betroffenen Klasse der Übertragung zustimmen würden. Diese könnten jedoch nach Art. 7 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) jederzeit ihre Einwilligungen widerrufen.
Zusätzlich wurde daher geprüft, ob eine Rechtsgrundlage für die Datenverarbeitung bei dieser Form der Liveübertragung gegeben ist. Der Thüringer Gesetzgeber beschloss mit dem Gesetz zur Weiterentwicklung des Schulwesens eine Regelung, die es den Schülern, welche den

regulären Unterricht nicht besuchen können, ermöglicht, die moderne Datenkommunikation zu nutzen, soweit die personellen und sachlichen Voraussetzungen vorliegen oder geschaffen werden können. Dies wurde im Schulgesetz in § 54 Abs. 7 aufgenommen. Damit wird zwar die Nutzung der digitalen Lernumgebungen rechtlich einbezogen und an die digitalen Herausforderungen angepasst, doch die Übertragung personenbezogener Daten Dritter, also die Liveübertragung der Lehrer und Schüler aus den Klassenzimmern, ist durch die Regelung nicht abgedeckt. Weder ist dies dort explizit genannt, noch kann dies bei Interpretation im Lichte der DS-GVO gewollt sein, da dies dem Grundsatz der Erforderlichkeit der Datenübermittlung widersprechen würde.
Der TLfDI steht dem möglichen Einsatz von Liveübertragungen sehr skeptisch gegenüber und sucht nach anderen Lösungen.

3.28 Automatisiertes Verfahren soll Schultagebuch für Kinder beruflich Reisender ersetzen

„DigLu“ – Digitales Lernen unterwegs – ist ein digitales Lernmanagementsystem für Kinder beruflich Reisender, mit dem das bisher in Papierform geführte Schultagebuch zunächst auf freiwilliger Basis ersetzt werden soll. Die Geeignetheit der dazu getroffenen organisatorischen und technischen Maßnahmen hat der TLfDI geprüft und wird das Verfahren auch während der Pilotphase weiter begleiten.

Kinder von beruflich Reisenden sind von häufigen Ortswechseln ihrer Eltern mit betroffen und müssen zur Erfüllung ihrer Schulpflicht immer wieder andere Schulen besuchen. Einem kontinuierlichen und individuellen Lernen sind damit Grenzen gesetzt, weil die betroffenen Schülerinnen und Schüler immer von anderen Lehrkräften betreut werden. Um eine Übersicht über die Unterrichtsinhalte und den Leistungsstand dieser Kinder zu bekommen, hatten sich alle Bundesländer in der Kultusministerkonferenz (KMK) darauf geeinigt, ein sogenanntes Schultagebuch einzuführen, welches jedes Kind führen muss. Das Schultagebuch enthält die Stammdaten des Kindes und der Eltern, eine Chronik über die besuchten Schulen, Lernpläne in einigen Kernschulfächern: es ist Grundlage zur Leistungsbewertung und Erstellung der Zeugnisse und dient darüber hinaus als Kommunikations- und Dokumentationsinstrument für die Schule, die Eltern sowie die Schülerinnen und Schüler. Daneben wird durch die Anwesenheitsbestätigung

der Schule der Nachweis erbracht, dass die Schulpflicht auch tatsächlich erfüllt wird. Die Nachteile des in Papierform geführten Schultagebuchs sind offensichtlich. Mit einem Verlust dieses Buches oder eingehefteter Seiten hieraus gehen zahlreiche Informationen über das Schulkind verloren. Eine Rekonstruktion ist nur äußerst mühsam durchführbar. Ebenso gerät die Funktion des Buches bei Auslandsaufenthalten als Lernunterstützung an seine Grenze. Oftmals werden die Kinder in solchen Situationen nicht beschult und eine Unterstützung oder Unterricht per Telefon und E-Mail von der für das Kind zuständigen Stammschule am Hauptwohnsitz der Eltern gestaltet sich zäh. Zur Verbesserung dieser Situation wurde von einigen Ländern aus dem Schulausschuss der KMK heraus den Datenschutzaufsichtsbehörden ein Konzept zur Prüfung vorgestellt, bei dem die Führung des Schultagebuchs durch eine digitale Schul- und Verwaltungsplattform „DigLu“ – Digitales Lernen unterwegs – ersetzt werden soll. Es gründete sich hierzu eine Unterarbeitsgruppe aus dem Kreis der Datenschutzaufsichtsbehörden unter der Federführung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). In mehreren Sitzungen wurden die verschiedenen datenschutzrechtlichen Aspekte zu „DigLu“ gesammelt und Forderungen gegenüber der KMK-Arbeitsgruppe formuliert. Insbesondere das von den KMK-Vertretern entworfene Datenschutzkonzept zu „DigLu“ war Anlass für eine umfassende datenschutzrechtliche Kritik. Da das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) sich dieses Themas besonders angenommen hat, führte der TLfDI mehrere Beratungsgespräche mit dem TMBJS zur Umsetzung der datenschutzrechtlichen Forderungen. Diese Änderungs- und Ergänzungshinweise fanden ihren Niederschlag in den zu „DigLu“ erstellten Unterlagen. Aus datenschutzrechtlicher Sicht hat der TLfDI nunmehr gegen die testweise Einführung von „DigLu“ keine Bedenken mehr erhoben.
Im Ergebnis soll nach jetzigem Stand (Dezember 2019) „DigLu“ als länderübergreifendes Pilotprojekt in den Pilotländern Baden-Württemberg, Bayern, Hessen, Niedersachsen, Nordrhein-Westfalen, Sachsen und Thüringen im Jahr 2020 starten. Während, wie oben beschrieben, die Führung des Schultagebuchs für die betroffenen Eltern beziehungsweise die Kinder verpflichtend ist, kann die Teilnahme an „DigLu“ mangels einer Rechtsvorschrift nur auf freiwilliger Basis erfolgen. Die Erziehungsberechtigten müssen deshalb zuvor in die Teilnahme schriftlich einwilligen.

Die Vorteile, die sich die beteiligten Kultusministerien von dem digitalen Verfahren im Gegensatz zum schriftlich zu führenden Tagebuch versprechen, sind ein kontinuierliches Unterrichten des Kindes sowie die Beobachtung der Lernentwicklung unabhängig vom konkreten Aufenthaltsort. Die Stammschule kann beispielsweise dem Kind Lernmaterial über eine Cloud zur Verfügung stellen, auf die das Kind beziehungsweise dessen Eltern Zugriff erhalten. Auf diesem Weg können die Schülerinnen und Schüler erledigte Hausaufgaben den zuständigen Lehrkräften zur Korrektur abgeben. Ein großer Vorteil ist das Entfallen der Problematik eines Verlustes des Schultagebuchs, da alle relevanten Daten zentral auf Servern gespeichert werden. Ab 1. August 2020 wird eine Änderung im Thüringer Schulgesetz (ThürSchulG) inkraft treten, wonach gemäß § 54 Abs. 7 ThürSchulG der Unterricht in besonderen Fällen (Schulpflichtige halten sich für längere Zeit in einer medizinischen Einrichtung oder einer Jugendarrestanstalt auf oder können aus anderen Gründen länger nicht am Unterricht in der Schule teilnehmen) mit Zustimmung des für das Schulwesen zuständigen Ministeriums ganz oder teilweise in digitalen Lernumgebungen stattfinden kann. Der TLfDI wird das beschriebene Verfahren weiterhin in der Pilotphase begleiten und bei möglichen datenschutzrechtlichen Problemen, die sich in der Praxis zeigen können, entsprechend eingreifen.

3.29 E-Mail-Adressen für Thüringer Lehrkräfte elektronisch kommunizieren – aber sicher!

Beim schulischen Nachrichtenaustauch zwischen Lehrkräften und Eltern sind naturgemäß oft personenbezogene Daten im Spiel. Der TLfDI wirkt an einer Lösung für die E-Mail-Kommunikation Thüringer Schulen mit, die sowohl datenschutz- als auch nutzerfreundlich ist.

E-Mails gehören lange schon zum Alltag und haben auch in Messenger-Zeiten noch ihren festen Platz. Während WhatsApp, Signal und Threema und so weiter besonders fürs private Chatten üblich sind, ist die E-Mail zwischen Firmen und Privatkunden und zwischen Bürgern und Behörden meist die erste Wahl, wenn es darum geht, Nachrichten schnell und papierlos auszutauschen. Vielfach ist dabei nicht im Blick, dass auf dem Übertragungsweg vom Absender bis zum Empfänger vertrauliche Mailinhalte auf Abwege geraten können. Das gilt auch trotz der heute üblichen Transportverschlüsselung, denn eine normale

E-Mail wird beim Provider unverschlüsselt gespeichert. Abhilfe schafft hier nur eine Ende-zu-Ende-Verschlüsselung. Das heißt, dass die E-Mail auf dem Gerät (Laptop, Smartphone) des Absenders verschlüsselt und erst auf dem Gerät des Empfängers wieder entschlüsselt wird. Eine solche Verschlüsselung gewährleistet, dass die Nachricht nicht von Dritten gelesen oder gar verändert werden kann. OpenPGP und S/MIME sind hier standardisierte technische Lösungen, die aber von den Nutzern bei der Einrichtung und Schlüsselverwaltung einigen Aufwand erfordern. Deshalb werden sie nur wenig eingesetzt.
Für Thüringer Lehrkräfte, die sowohl untereinander als auch mit Eltern und Schülern schulbezogen kommunizieren wollen, ist ein Kompromiss in Sicht, an dem auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mitgewirkt hat. Alle Lehrkräfte sollen im Schuljahr 2019/2020 eine dienstliche E-Mail-Adresse erhalten und ihre Nachrichten auch zu Externen (Eltern, Schülern) sicher übertragen können. Kern des Systems ist die Kombination aus moderner Transportverschlüsselung und OpenPGP-Verschlüsselung auf dem Mailserver. Die Mails werden im browserbasierten Webmailer geschrieben, sicher versendet und empfangen. Zudem erfolgt automatisch eine PGP-verschlüsselte Speicherung auf dem Server. Der Charme an der Sache: Sender und Empfänger müssen sich lediglich ihr selbstgewähltes Passwort merken, das beim Abholen der E-Mail für Entschlüsselung sorgt. Alles andere passiert im Hintergrund. Vor Einführung des Systems sind noch Detailfragen zu klären, zum Beispiel, welche dienstlichen Inhalte über dieses System übertragen werden dürfen und welche nicht. Schließlich sind die Mails hier nicht nach der reinen Lehre Ende-zu-Ende-verschlüsselt. Das Risiko ist für eine Einladung zur Elternversammlung anders zu bewerten als für ein sonderpädagogisches Gutachten, welches den Eltern per Mail zugeleitet werden soll. Der TLfDI wird den Prozess weiter aktiv begleiten und hofft mit vielen Lehrerinnen und Lehrern, dass bald eine Lösung erreicht wird, die sowohl nutzerfreundlich als auch datenschutzgerecht ist. Es geht schließlich um personenbezogene Daten von Kindern und Jugendlichen. Da wird der TLfDI besonders genau hinschauen.

3.30 Schuldaten auf dem Privat-PC eines Lehrers. Ist das zulässig?

Darf ein Lehrer einer staatlichen Schule auf seinem Privatcomputer Zeugnisse erstellen? Ja, aber nur unter sehr strengen Bedingungen.

Eine Lehrkraft einer staatlichen Schule fragte nach, ob sie auf ihrem Privatcomputer mit Internetzugang Programme zur Notenverwaltung beziehungsweise Zeugniserstellung für die Schule nutzen dürfe. Des Weiteren wollte sie wissen, ob es bestimmte Bedingungen gäbe, die eingehalten werden müssten, um ein solches Programm auf dem Privatcomputer zu verwenden.
Zunächst ist klarzustellen, dass es keine Verpflichtung des Lehrers gibt, Zeugnisse zu Hause auf privaten Endgeräten zu erstellen. Entsprechend einem Schreiben vom Thüringer Kultusministerium im Mai 2000 an die staatlichen Schulämter muss zudem jede Lehrkraft, die einen privaten Rechner für die Erledigung schulischer Aufgaben nutzen und dabei personenbezogene Daten der Schüler verarbeiten will, dies vorher ihrer Schule mitteilen und eine Genehmigung einholen. Auch wenn dies vor der Datenschutz-Grundverordnung (DS-GVO) war, so bleibt weiterhin die Schule die verantwortliche Stelle. Sollte ein Lehrer diese Tätigkeiten zu Hause auf privaten Endgeräten verrichten wollen und sollte dies genehmigt sein, ist der nachfolgende Weg datenschutzrechtlich zulässig:
Die Schule kann zum Beispiel einen USB-Stick zur Verfügung stellen, auf dem die Vordrucke enthalten sind und auf dem die erstellten Zeugnisse abgelegt werden können. Zudem müssen die nachfolgenden Punkte beachtet werden:

a) Werden personenbezogene Daten, wie zum Beispiel Zeugnisse, auf dem USB-Stick gespeichert, müssen diese Daten verschlüsselt sein. Ausführliche Hinweise zur Umsetzung finden sich auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik unter www.bsi.bund.de bei Eingabe des Suchbegriffs Verschlüsselung (Link: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/datenverschluesselung_node.html).

b) Bei der Arbeit am heimischen Rechner dürfen die personenbezogenen Dateien nur auf dem USB-Stick gespeichert werden.
c) Wenn nicht an den Dateien gearbeitet wird, muss mit einer aktiven Verschlüsselung sichergestellt werden, dass kein Zugriff auf die Daten durch Dritte erfolgen kann.
d) Der Transport beziehungsweise die Übermittlung der Dateien zur Schule darf auch nur verschlüsselt erfolgen. Ein Versand von ausgefüllten Zeugnissen per E-Mail wäre nur erlaubt, falls die Daten tatsächlich Ende-zu Ende-verschlüsselt übertragen werden. Da dies derzeit in der Regel nicht der Fall ist, muss vom elektronischen Versand abgesehen werden. Diese Ansicht vertritt auch das Ministerium für Bildung, Jugend und Sport in seiner Broschüre „Antworten auf häufig gestellte Fragen zum Datenschutz in Schulen“, mit Stand Oktober 2019 unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/schule/faq_datenschutz_in_schulen.pdf.

Falls in Thüringen zukünftig eine durch öffentliche Stellen betriebene Schul-Cloud nutzbar wird, wäre zu klären, inwieweit weitere Möglichkeiten der Verarbeitung zulässig wären. Diese Entwicklung wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit im Auge behalten und als Aufsichtsbehörde beratend begleiten.

3.31 Schule stellt teilweise sensible personenbezogene Daten von Schülern und Eltern ins Internet

Die von den Schulen zu verarbeitenden Angaben der Schülerinnen und Schüler zur Herstellung des Kontaktes in Notfällen müssen in automatisierter Form geführt werden, damit in solchen Krisen- und Notfällen das zuständige Schulamt diese Daten im automatischen Verfahren abrufen kann. Die Schule hat dabei sicherzustellen, dass niemand unbefugt auf diese teilweise sensiblen personenbezogenen Daten zugreifen kann.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt telefonisch die Mitteilung, dass im Internetauftritt einer Regelschule umfangreiche personenbezogene Da-

ten von Schülerinnen von Schülern der Schule öffentlich sichtbar wären. Wie sich der TLfDI selbst überzeugen konnte, waren listenmäßig nach Klassen geordnet Klassenlehrer, Nachnamen, Vornamen, Geburtsdatum, Wohnanschriften, Telefonnummern sowie Ansprechpartner einschließlich deren Telefonnummern angegeben.
Da der Hinweis auf diese Seite in den Sommerferien erfolgte, konnte in der Schule niemand kurzfristig erreicht werden. Eine ebenfalls sofort gesendete E-Mail an die Schule blieb ebenso unbeantwortet. Der Schule wurde darin erläutert, dass es sich um eine Verletzung des Schutzes personenbezogener Daten handelt und die Schule als Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) gemäß Art. 33 DS-GVO verpflichtet ist, dem TLfDI eine Meldung über diese Verletzung zu machen. Der TLfDI empfiehlt, hierfür das von ihm auf seiner Internetseite unter https://www.tlfdi.de/mam/tlfdi/datenschutz/meldung_datenpanne_.docx abrufbare Formular zu verwenden. Die Schule wurde zusätzlich aufgefordert, die Datei im Internet zu löschen beziehungsweise den öffentlichen Zugriff über die Webseite zu unterbinden. Da die entsprechende Information auch über eine Google-Suche gefunden wurde, wurde die Schule auch ersucht, bei Google einen dort zur Verfügung gestellten Löschantrag einzureichen. Dieser Löschantrag richtet sich darauf, dass bestimmte Ergebnisse aus der Google-Suche entfernt werden.

Weil die sofortige Ansprache der Schule keinen Erfolg zeigte, wurde das zuständige Staatliche Schulamt über den Vorfall ebenfalls unterrichtet und gebeten mitzuteilen, welche Möglichkeiten der kurzfristigen Kontaktaufnahme mit der Schule bestehen. Wie das Staatliche Schulamt dem TLfDI mitteilte, konnte der Schulleiter erreicht werden und über den vom TLfDI beschriebenen Sachverhalt unterrichtet werden. Dieser teilte dem TLfDI mit, dass die Schule die Excel-Datei mit den personenbezogenen Daten der Schülerinnen und Schüler gelöscht habe und die Betroffenen schriftlich über den Vorfall unterrichtet würden. Der TLfDI bewertete den Sachverhalt gegenüber dem Schulleiter als datenschutzrechtlichen Verstoß, sah aber zu diesem Zeitpunkt, da der Mangel als kurzfristig beseitigt anzusehen war, von einer weiteren Ausübung seiner Sanktionsmöglichkeiten ab.

Dann aber musste der TLfDI feststellen, dass entgegen den Angaben des Schulleiters nach wie vor der Zugriff im Internet auf die oben genannte Excel-Datei bestand. Der TLfDI bewertete nun die fortdauernde Verletzung von datenschutzrechtlichen Vorschriften als schweren datenschutzrechtlichen Verstoß, der unverzüglich zu beheben war. Der TLfDI erließ daraufhin einen Bescheid, in dem nach Art. 58 Abs. 2 Buchstabe b) Datenschutz-Grundverordnung gegen die Schule, vertreten durch die Schulleitung, eine Verwarnung ausgesprochen wurde. Der Bescheid ging nachrichtlich an das Thüringer Ministerium für Bildung, Jugend und Sport sowie das zuständige Schulamt. Als dann eine Woche, nachdem erneut die Behebung des Mangels durch den Schulleiter mitgeteilt worden war, der TLfDI eine Beschwerde von Eltern bekam, wonach im Internet nach wie vor die personenbezogenen Daten ihres Kindes abrufbar seien, erfolgte noch am selben Tag von Mitarbeitern des TLfDI eine Vor-Ort-Kontrolle dieser Schule. Wie sich zeigte, war zwar die Excel-Datei inzwischen tatsächlich im Internet gelöscht worden, allerdings lagen nach wie vor Teile der Datei in einem Zwischenspeicher der Google-Suchmaschine. Die Mitarbeiter des TLfDI riefen daraufhin auf dem PC des Schulleiters eine Website bei Google auf, mit der bei Google ein Antrag auf Löschung solcher nach wie vor dort gespeicherten Inhalte gestellt wurde. Bereits zwei Tage später konnte der TLfDI feststellen, dass keine personenbezogenen Daten mehr bei der Eingabe der Internetadresse, die zur Excel-Datei führte, abgerufen werden konnten. Der Fall konnte erst ab diesem Zeitpunkt als abgeschlossen angesehen werden. Darüber hinaus wies der TLfDI den Schulleiter allerdings auch darauf hin, dass gemäß § 136 Abs. 4 Thüringer Schulordnung in den Klassen- oder Kursbüchern Angaben zur Herstellung des Kontakts in Notfällen aufgeführt werden und zusätzlich nach Abs. 10 „das zuständige Schulamt die für die Klassen- oder Kursbücher nach Absatz 4 Satz 2 Nr. 1 bis 3 und 8 erhobenen Daten im automatisierten Verfahren abrufen“ kann. Daher müssen die Schulen für Krisen- oder Notfälle sogar eine solche Liste in automatisierter Form führen. Sie sind allerdings verpflichtet, Zugriffe auf diese Datei durch Personen, die die personenbezogenen Daten nicht zur Aufgabenerfüllung benötigen, durch das Ergreifen der geeigneten organisatorischen und technischen Maßnahmen auszuschließen.

3.32 Akteneinsicht oder Kopie der Akte? Was sagen Datenschutzgrundverordnung und das Verwaltungsverfahrensgesetz?

Nach der Datenschutz-Grundverordnung kann Auskunft über die bei einem Verantwortlichen gespeicherten personenbezogenen Daten verlangt werden. Ein Recht auf Akteneinsicht existiert nach diesem Gesetz nicht. Ein solches kann nach § 29 Thüringer Verwaltungsverfahrensgesetz geltend gemacht werden. Dies ist allerdings kostenpflichtig.

Zwischen den Eltern eines Schülers und seiner Schule entstand ein Streitverhältnis. Infolgedessen begehrten die Eltern Einsicht in die Schülerakte. Die Schule wies darauf hin, dass dies Kosten nach der Verwaltungskostenordnung, § 1 Thüringer Verwaltungskostengesetz in Verbindung mit der Anlage 1 zur Thüringer Allgemeinen Verwaltungskostenordnung, verursachen würde. Die Kosten werden angesetzt für die Arbeitszeit der Beaufsichtigung, während der die Akteneinsicht stattfindet, und gesondert für Kopien, die aus der Akte gemacht werden sollen. Diese Kosten wollten die Eltern nicht tragen.
Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) beantragten sie, dass er sich dafür einsetzen solle, dass Akteneinsicht kostenfrei gewährt würde.
Der TLfDI erteilte folgende Rechtsauskunft:
Nach Art. 15 Abs. 1 und 3 Datenschutz-Grundverordnung (DS-GVO) haben die Eltern (beziehungsweise die Kinder, vertreten durch die Eltern) einen Anspruch auf Auskunftserteilung, welche Art von Daten über sie gespeichert sind (Abs. 1), und nach Abs. 3 können sie auch Kopien der über sie gespeicherten Daten verlangen. Bei der ersten Nachfrage hat dies kostenfrei zu erfolgen. Ein Recht auf Akteneinsicht besteht nach dieser Vorschrift und insgesamt in der DS-GVO nicht.
Akteneinsicht kann durch Beteiligte in einem Verwaltungsverfahren nach § 29 Thüringer Verwaltungsverfahrensgesetz bei der Behörde, hier die Schule, beantragt werden. Da es sich dabei um eine Leistung einer öffentlichen Stelle handelt, hat diese das Thüringer Verwaltungskostengesetz anzuwenden.
Für die Rechtmäßigkeit der Erhebung von Gebühren für die Akteneinsicht wird zum Beispiel auf das Urteil des Verwaltungsgerichts Karlsruhe vom 26. Juli 2011 – 6 K 2797/10 verwiesen.

Der Rat des TLfDI lautete daher, sich auf Art. 15 Abs. 3 DS-GVO zu berufen.
Gegenstand des Anspruchs sind die auf die Person bezogenen Daten, die bei dem Verantwortlichen zum Zeitpunkt der Auskunftserteilung vorhanden sind. Die Datenkopie muss vollständig sein. Das Recht der betroffenen Person beschränkt sich allerdings auf eine Kopie der sie betreffenden personenbezogenen Daten. Personenbezogene Daten von Dritten sind unkenntlich zu machen.

3.33 Kommunales Haushaltsrecht und Betriebskosten im Kindergarten: Keine Rechnungsprüfung ohne Daten

Die Übermittlung von personenbezogenen Daten einer Kindertageseinrichtung in freier Trägerschaft an die Kommunalverwaltung ist zum Zwecke der haushalterischen Rechnungsprüfung der Betriebskostenabrechnung grundsätzlich zulässig. Rechtsgrundlage für die Übermittlung ist § 17 Abs. 1 Satz 1 Nr. 3 Thüringer Datenschutzgesetz (ThürDSG). § 17 Abs. 1 Satz 1 Nr. 3 ThürDSG bestimmt, dass eine Änderung des Zweckes, für den die Daten ursprünglich erhoben wurden, für die Rechnungsprüfung der Betriebskostenabrechnung des Trägers der Kindertageseinrichtung zulässig ist.

Im Berichtszeitraum wandte sich ein externer betrieblicher Datenschutzbeauftragter (bDSB) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass eine Thüringer Gemeinde vom freien Träger einer Kindertageseinrichtung der Gemeinde verlangte, personenbezogene Daten der betreuten Kinder an die Gemeindeverwaltung zu übermitteln.
Nach Angaben des bDSB verlangte die Gemeinde vom Kindergartenträger eine monatliche Auflistung der betreuten Kinder mit Namen, Geburtsdaten und Anschriften, gestaffelt nach Alter der Kinder (0 bis 2, 2 bis 3 Jahre und so weiter). Eine Übermittlung anonymisierter Namenslisten sei von der Gemeinde abgelehnt worden. Der bDSB legte dar, dass die Übermittlung namentlicher Kinderlisten an die Gemeinde zur Überprüfung der Betriebskostenabrechnung nicht rechtskonform sei, da sich weder aus § 21 Abs. 4 sowie § 22 Thüringer Kindertagesbetreuungsgesetz (ThürKitaG) noch aus dem Vertrag des KITA-Trägers mit der Gemeinde (im Vertrag § 3 – Meldepflicht) eine Rechtsgrundlage zur namentlichen Meldung der betreuten Kinder er-

gebe. Daher sei aus seiner Sicht eine anonyme Meldung für Kinder, deren Wohnsitz außerhalb der betreffenden Gemeinde liege, ausreichend und die Forderung der Gemeinde verstoße gegen den Datenschutz.
Nach Annahme des bDSB verstieß die Forderung der Gemeinde zudem gegen das Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchstabe c) der Datenschutz-Grundverordnung (DS-GVO), wonach Datenverarbeitungen „dem Zweck angemessen und (…) auf das die Zwecke der Verarbeitung notwendige Maß beschränkt" sein müssen.
Der bDSB bat den TLfDI um Mitteilung, ob der freie Träger der Kindertageseinrichtung verpflichtet sei, die geforderten personenbezogenen Daten der Kinder an die Gemeinde zu übermitteln. Auf Anforderung des TLfDI gab die Gemeinde eine Stellungnahme zur Anforderung der personenbezogenen Daten ab.
Nach § 21 Abs. 4 und Abs. 5 sowie § 22 ThürKitaG haben Gemeinden, in deren Gebiet die Kindertageseinrichtungen liegen, den durch die Elternbeiträge und den möglichen Eigenanteil des KITA-Trägers nicht gedeckten Anteil der erforderlichen Betriebskosten zu zahlen. Diese Zahlungen erfolgen auf der Grundlage der tatsächlich monatlich angemeldeten Kinder in der KITA. Die Höhe der zu leistenden Zahlungen ist abhängig von der Anzahl und vom Alter der Kinder. Daher ist das Geburtsdatum der Kinder erforderlich, um den tatsächlich zu zahlenden Betrag der Gemeinde für den entsprechenden Monat richtig zu berechnen.
Gemäß § 5 Abs. 1 ThürKitaG haben Eltern das Recht, ihr Kind auch in der Kindertageseinrichtung einer anderen Gemeinde als der Wohnsitzgemeinde betreuen zu lassen. Sofern das Kind aufgrund dieses Wunsch- und Wahlrechts in einer anderen Gemeinde als der Wohnsitzgemeinde betreut wird, hat die Wohnsitzgemeinde des Kindes der betreuenden Gemeinde gemäß § 21 Abs. 5 in Verbindung mit § 22 Abs. 2 ThürKitaG die monatlichen Betriebskosten zu zahlen.
Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO ist die Datenverarbeitung rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Nach § 17 Abs. 3 Satz 3 Sozialgesetzbuch I in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) DS-GVO kann der öffentliche Träger der Kindertageseinrichtung die zweckentsprechende Verwendung der öffentlichen Mittel nachprüfen. Zu diesem Zweck kann er konkrete Mitteilungen, Auskunft und Rechenschaft vom freien Träger

verlangen. Dies schließt naturgemäß die genaue Besetzung der KITA-Plätze anhand von Namen, Geburtsdaten und Anschriften der Kinder ein, um Falschmeldungen und Über- oder Unterzahlungen auszuschließen.
Alter und Anzahl der Kinder sind zudem für die Beantragung der Landespauschale gemäß § 25 ThürKitaG erforderlich, Alter und Wohnsitz der Kinder für die Forderung der monatlichen Betriebskosten von Fremdgemeinden gemäß § 21 Abs. 5 ThürKitaG. Sowohl die Zahlungen der gemeindlichen Betriebskostenanteile als auch die Zahlungen der Landespauschale gemäß § 25 Abs. 1 ThürKitaG und die Zahlungen aufgrund des wahrgenommenen Wunsch- und Wahlrechts unterliegen der Rechnungsprüfung im Rahmen des kommunalen Haushaltsrechts. Somit benötigt die Gemeinde auch hierfür die genaue Anzahl der Kinder, deren Alter und deren Wohnsitz. Da gemäß § 17 Abs. 1 Satz 1 Nr. 3 ThürDSG als Zweck der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen neben den ursprünglichen Zwecken immer auch die Verarbeitung der Daten zur Rechnungsprüfung gilt, stellt die Forderung der Gemeinde zur Übermittlung der personenbezogenen Daten der betreuten Kinder keinen Verstoß gegen den Datenschutz dar.
Ein Datenschutzverstoß war daher nicht festzustellen.

3.34 Forschungsprojekt „Sicherheit und Kriminalität in Deutschland“ (SKiD)

Nach § 46 Bundesmeldegesetz (BMG) darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (Gruppenauskunft) unter der Beachtung der Zweckbindung nach § 47 BMG nur erteilt werden, wenn sie im öffentlichen Interesse liegt.

Im Berichtszeitraum wandte sich die Thüringer Polizei mit einer datenschutzrechtlichen Anfrage zum Forschungsprojekt „Sicherheit und Kriminalität in Deutschland“ (SKiD) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Befragung SKiD ist eine bundesweite Opferbefragung, die ab dem Jahr 2020 alle zwei Jahre durchgeführt werden soll. Insbesondere sollte der TLfDI klären, ob es sich bei der Durchführung der Feldarbeit durch ein Umfrageinstitut um eine Auftragsverarbeitung für das Bundeskriminalamt (BKA) handle. Die Adressen der Befragten für die Stichproben sollen durch das jeweilige Bundesland für das BKA

bei den dortigen Einwohnermeldeämtern aus der Einwohnermeldedatei eingeholt und dann über das BKA direkt an das Umfrageinstitut übermittelt werden. Dabei tritt das betreffende Landeskriminalamt nicht selbstständig, sondern nur als ausführendes Organ des BKA auf. Des Weiteren bat die Thüringer Polizei den TLfDI um Mitteilung einer melderechtlichen Rechtsgrundlage für die Herausgabe der Adressdaten durch die Einwohnermeldeämter.
Nach Ansicht des TLfDI sollte hier der Umweg über eine eventuelle Auftragsverarbeitung zwischen dem BKA, dem Thüringer Landeskriminalamt (TLKA) und dem Umfrageinstitut vermieden werden. Zielführender war nach Ansicht des TLfDI eine direkte Abfrage der Adressen durch das Umfrageinstitut bei den jeweiligen Einwohnermeldeämtern. Nach § 46 Bundesmeldegesetz (BMG) darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (Gruppenauskunft) unter der Beachtung der Zweckbindung nach § 47 BMG nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Danach müssen die Personen, über die Auskunft begehrt wird, nicht namentlich bezeichnet, sondern nur durch vom Auskunftsersuchenden anzugebende Merkmale abstrakt beschrieben werden. Die in Frage kommenden Personen haben mindestens ein im Melderegister gespeichertes Merkmal gemeinsam (zum Beispiel Bewohner einer bestimmten Straße, alle minderjährigen Bewohner einer Gemeinde), aus dem sich die Zusammensetzung der Personengruppe, die Gegenstand der Auskunft wird, erst ergibt. Voraussetzung für die Zulässigkeit einer Gruppenauskunft ist, abgesehen von dem Vorliegen einer Auskunftssperre nach den §§ 51 und 52 BMG, dass sie im öffentlichen Interesse liegt. Der Begriff des öffentlichen Interesses ist – wie der des berechtigten beziehungsweise rechtlichen Interesses – ein unbestimmter Rechtsbegriff und somit gerichtlich voll nachprüfbar. Unter öffentlichem Interesse ist vor allem das Interesse der Allgemeinheit zu verstehen, das sich insoweit vom Individualinteresse einzelner Personen oder Gruppen grundsätzlich unterscheidet und über das berechtigte Interesse einzelner Auskunftssuchender hinausgeht. Ein öffentliches Interesse für die Erhebung durch das Umfrageinstitut könnte vorliegend in der Erstellung einer Kriminalitätsstatistik liegen. Bei diesem Verfahren müsste das TLKA nicht als Informationsbeschaffer „zwischengeschaltet“ werden. Auch verstößt eine Direktabfrage der Umfrageinstitute nicht gegen den Grundsatz der Direkterhebung aus Art. 6 und Art. 8 Charta der Grundrechte der Europäischen Union. Nach dem Di-

rekterhebungsgrundsatz sind personenbezogene Daten vorrangig beim Betroffenen zu erheben.
Die Beurteilung, ob zwischen dem BKA und dem Umfrageinstitut ein Vertrag zur Auftragsverarbeitung geschlossen werden muss, unterfällt der Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Dies teilte der TLfDI der Thüringer Polizei mit.

3.35 Der Personalausweis ist kein Pfandmittel

Der Personalausweis darf nicht als Pfandmittel eingesetzt werden. Dies ergibt sich aus § 1 Abs. 1 Satz 3 Personalausweisgesetz. Daher darf auch ein Museum für das Ausleihen eines Audioguides nicht die Hinterlegung des Personalausweises als Pfand verlangen. Das entspricht gerade nicht „geltendem Recht".

Eine Besucherin der Alten Synagoge in Erfurt beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass Besucher ihren Personalausweis hinterlegen müssten, um einen Audioguide ausleihen zu können. Einen als Pfand angebotenen Geldbetrag oder andere Möglichkeiten lehnte das Museum ab.
Auf Nachfrage des TLfDI erklärte die Stadtverwaltung Erfurt, die Hinterlegung des Personalausweises geschehe als Pfand „auf der Grundlage geltendes Rechts".
Diese Auffassung teilt der TLfDI nicht. § 1 Abs. 1 Satz 3 Personalausweisgesetz regelt unmissverständlich, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Folglich durfte hier im konkreten Fall vom Museum nicht verlangt werden, den Personalausweis als Pfandmittel für einen Audioguide zu hinterlegen.
Der TLfDI wies auf diesen Verstoß hin und bat eindringlich, diese Praxis künftig zu unterlassen. Da der TLfDI Verständnis dafür hatte, dass das Museum sich gegen Diebstahl absichern wollte, regte er an, Geldbeträge (ab 20 Euro) hinterlegen zu lassen. In der Nähe des Museums befinden sich Bankautomaten. Die Besucher können somit ohne größeren Aufwand entsprechende Geldbeträge abheben.
Die Erfurter Stadtverwaltung setzte den Hinweis umgehend um. Die Besucher können sich nun mit den ausgestellten Gegenständen jüdi-

schen Lebens in Erfurt beschäftigen, ohne Angst um ihre personenbezogenen Daten haben zu müssen.

3.36 Datenschutz im digitalen Zeitalter: telemedizinische Versorgung von Schlaganfallpatienten

Seit 2012 werden im Universitätsklinikum Jena Schlaganfall-Patienten über das „Schlaganfall Telemedizin Netzwerk in Thüringen“ (SATELIT) akut-medizinisch versorgt. Insbesondere Patienten, die nicht in der direkten Umgebung einer spezialisierten Klinik leben, erhalten über SATELIT schnelle medizinische Hilfe. Dennoch muss auch bei digitalen medizinischen Maßnahmen die Sicherheit der Datenflüsse gewährleistet sein.

Gerade bei Schlaganfall-Patienten sind die schnelle Diagnose und der unverzügliche Beginn der richtigen Behandlung entscheidend, um das Ausmaß der Folgeschäden so gering wie möglich zu halten. Für die rettende Behandlung dürfen nicht erst Stunden durch den Transport zu einer Spezialklinik vergehen. Medizinisch wie technisch ist eine zeitnahe Behandlung ein großer gesundheitlicher Gewinn für die betroffenen Patienten.
Im Schlaganfall Telemedizin Netzwerk in Thüringen (SATELIT) stehen drei neurologische Schlaganfall-Zentren (Klinikum Altenburger Land, HELIOS Klinikum Erfurt und das Universitätsklinikum Jena) miteinander und mit weiteren Kliniken in Thüringen in Verbindung. Durch und über dieses Netzwerk wird Expertenwissen gebündelt und kann von den beteiligten Kliniken ohne Zeitverlust abgerufen werden. Die Schlaganfallspezialisten können im Netzwerk per Video direkt mit dem Patienten und mit dem Ärzteteam vor Ort kooperieren; ein neurologischer Facharzt ist hierfür rund um die Uhr erreichbar. Per Video und durch den Austausch von CT- und MRT-Bildern kann er Schlaganfallsymptome wie Lähmungen, Koordinations- und Sprachstörungen sofort analysieren. Damit werden über das Netzwerk umfassende sensible Gesundheitsdaten von Patienten zwischen den beteiligten Kliniken übermittelt und medizinisch ausgewertet.
Gesundheitsdaten zählen gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) zu den besonderen Kategorien von Daten, die einem erhöhten Schutzniveau unterliegen. Um diese Daten vor dem unbefugten Zugriff durch Dritte zu schützen und eine unbefugte Verbreitung, insbesondere über das Internet, zu verhindern, sind gemäß

Art. 32 Abs. 1 und Abs. 2 DS-GVO umfassende technische und organisatorische Maßnahmen erforderlich. Diese Maßnahmen des Universitätsklinikums Jena (UKJ) hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner Aufsichtsfunktion datenschutztechnisch und datenschutzrechtlich geprüft. Eine vergleichbare Prüfung wird der TLfDI in absehbarer Zeit auch in den übrigen beteiligten Kliniken vornehmen.

In die Prüfung wurden auch die Auftragsverarbeitungsverträge (AVV) des UKJ mit den Kooperationspartnern von SATELIT einbezogen, das heißt der Vertrag mit der Technikfirma, die Produkte zur integrierten Schlaganfallmedizin herstellt, und der Vertrag mit den Partnerkliniken von SATELIT. Die Technikfirma führt auch die regelmäßigen Wartungsarbeiten am Server-System von SATELIT durch.

Im Rahmen der Prüfung gab der TLfDI verschiedene Hinweise und stellte Änderungsforderungen, um die Datensicherheit im gebotenen Maße zu gewährleisten. Das UKJ setzte die Änderungen sukzessive um. Ein zentraler Aspekt hierbei war, sicherzustellen, dass kein Angreifer in das Netzwerk, in dem die medizinischen Systeme betrieben werden, eindringen kann und Patientendaten auch im Falle eines erforderlichen Austauschs der Datenträger nicht von Unbefugten ausgespäht werden können. Im Sinne der Datensicherheit bei allen Kooperationspartnern wurden die Forderung eines regelmäßigen Passwortwechsels für den Systemzugang und die datenschutzgerechte Vernichtung von Datenträgern auch verbindlich in die AVV-Verträge aufgenommen. Dies galt ebenso für die Dokumentation der fachgerechten Entsorgung der Datenträger.

Für den passwortgeschützten Systemzugang wurde zudem das IT-Grundschutzkompendium Organisation und Personal (ORP), ORP.4.A8 zur „Regelung des Passwortgebrauchs“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts_und_Berechtigungsmanagement.html). Danach gilt für die Passwortnutzung Folgendes: „Die Institution muss den Passwortgebrauch verbindlich regeln. Dabei muss festgelegt werden, dass nur Passwörter mit ausreichender Länge und Komplexität verwendet werden. (…) Die Passwörter müssen sofort

gewechselt werden, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht. Passwörter müssen geheim gehalten werden. Standardpasswörter müssen durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert werden (…).“

Die Anforderungen des BSI wurden vom UKJ berücksichtigt und in der IT-Nutzerordnung sowie dem zugehörigen Regelwerk des UKJ verankert. Hierauf wurde auch in den AVV-Verträgen Bezug genommen.

Das UKJ betreibt darüber hinaus ein Informationssicherheitsmanagementsystem (ISMS) nach der ISO 27001 und trifft im Rahmen des IT-Sicherheitsgesetzes (§ 8a BSIG) angemessene organisatorische und technische Vorkehrungen, um Störungen der IT-Systeme und -Prozesse zu vermeiden. Die Regelung zur Passwortsicherheit ist an den Anhang A der ISO 27001 mit der Maßnahme A.9.3.1 „Gebrauch geheimer Authentisierungsinformation“ angelehnt und in der IT-Nutzerordnung des UKJ verankert. Die IT-Nutzerordnung ist zentral für alle Mitarbeiter des UKJ gültig und verbindlich. Sämtliche Benutzer sind verpflichtet, die Regelungen des UKJ zur Verwendung geheimer Authentisierungsinformationen zu befolgen. Alle Maßnahmen, die im Rahmen des ISMS umgesetzt wurden, orientieren sich an der ISO 27001. Die Zertifizierung wurde im Juni 2019 erfolgreich abgeschlossen.

Die Forderung des TLfDI, die Entsorgung von Festplatten und elektronischen Speichermedien mit Seriennummern durch das beauftragte Unternehmen zu protokollieren, wurde in der Richtlinie des UKJ zur „Entsorgung der Wiederverwendung von Geräten und Betriebsmitteln“ ebenfalls aufgenommen. Zur Nachvollziehbarkeit der Vernichtung wird außerdem gemäß Forderung des TLfDI ein Abgleich von Vernichtungsprotokollen mit den Inventarnummern der im Container befindlichen Speichermedien durchgeführt, um das unbefugte Entwenden von Datenträgern aus den Containern zu verhindern. Nachdem alle Prüfungen abgeschlossen waren, teilte der TLfDI dem UKJ Ende Oktober 2019 mit, dass beim Einsatz von SATELIT das hohe Schutzniveau der Gesundheitsdaten gewährleistet wird und die erforderlichen technischen wie organisatorischen Maßnahmen im Sinne der DS-GVO getroffen wurden.

3.37 Wie sicher ist „die Neue“?

Die Gesundheitskarte gibt es seit einigen Jahren. Nunmehr soll deren Funktion deutlich erweitert werden. Es sollen auch die Behandlungen dort dokumentiert und für die behandelnden Ärzte auslesbar seien. Dabei gibt es allerdings Probleme.

Im Jahr 2018 war das Wort „Datenschutz“ nicht nur aufgrund der Datenschutz-Grundverordnung (DS-GVO) in aller Munde. Auch die öffentliche Berichterstattung brachte immer wieder Fälle von Datenmissbrauch, Datenskandalen oder Hackerangriffen ans Licht. Es scheint, als habe der digitale Fortschritt auch seine Schattenseiten, nämlich, wenn Daten unbefugt ausspioniert, gesammelt oder zweckentfremdet werden. Bürgerinnen und Bürger äußern damit völlig zu Recht ihre Besorgnis in Bezug auf die Sicherheit ihrer Daten, besonders wenn es sich hierbei um sensible Daten wie ihre Gesundheitsdaten handelt.
Ein Bürger fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) berechtigterweise nach, wie sicher die neue Gesundheitskarte sei. Mit dem am 1. Januar 2004 inkraft getretenen Gesetz zur Modernisie-rung der gesetzlichen Krankenversicherung – GKV-Modernisierungsgesetz – wurde unter anderem in der Vorschrift § 291a Fünftes Buch Sozialgesetzbuch (SGB V) die Einführung der elektronischen Gesundheitskarte festgelegt (siehe 6. Tätigkeitsbericht [TB] des TLfDI, Punkt 11.4). Diese sollte künftig die Möglichkeit anbieten, umfangreiche medizinische Daten, zum Beispiel Medikationspläne der Patienten, elektronische Arztbriefe, einen Notfalldatensatz sowie eine elektronische Patientenakte und ein elektronisches Patientenpostfach (§§ 31a und 291a SGB V) auf der Karte zu speichern. Bis dahin konnten auf der Karte lediglich personenbezogene Basisdaten (Name, Geburtsdatum, Adresse) gespeichert werden. Seitdem berichtete der TLfDI regelmäßig über den Stand der elektronischen Gesundheitskarte, so zum Beispiel auch im 11. TB des TLfDI unter Punkt 15.8 „Happy Birthday – die elektronische Gesundheitskarte (eGK) wird 10 Jahre alt“.
Bei Gesundheitsdaten handelt es sich um besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO. Gemäß § 291b SGB V ist die Gesellschaft für Telematik für den Betrieb und die Weiterentwicklung der Telematikinfrastruktur, der elektronischen Gesundheitskarte sowie zugehöriger Fachanwendungen und sogenannter

weiterer Anwendungen für die Kommunikation zwischen Heilberuflern, Kostenträgern und Versicherten zuständig. Sie legt auch das Sicherheitskonzept, anzuwendende Dienste und Standards fest. Soweit bei den Festlegungen und Maßnahmen Fragen der Datensicherheit berührt sind, sind diese sogar im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik zu treffen. So hat die Gesellschaft für Telematik beispielsweise festgelegt, dass die elektronischen Gesundheitskarten der ersten Generation (G1) zum 31. Dezember 2018 ihre Gültigkeit verlieren und durch Karten der zweiten Generation (G2) ausgetauscht werden mussten. Dies wird wahrscheinlich auch nicht der letzte Wechsel gewesen sein, denn die eGK ist regelmäßig mit notwendigen Zertifikaten auszustatten und den höchsten Sicherheitsstandards dem Stand der Technik entsprechend anzupassen.

Auch sonst tut sich einiges. So sind niedergelassene Ärzte und Psychotherapeuten ab 1. Juli 2018 verpflichtet, ein sogenanntes Versichertenstammdatenmanagement (VSDM) zu nutzen. Dies dient der Online-Prüfung des Versichertennachweises. Im Rahmen dieser Prüfung soll durch eine geschützte direkte Online-Verbindung der Praxis mit den Krankenkassen in Echtzeit („online“) geprüft werden, ob die auf der eGK eines Patienten gespeicherten Versichertenstammdaten aktuell sind und ob ein gültiges Versicherungsverhältnis besteht. Für die Durchführung des VSDM werden verschiedene technische Komponenten und Dienste in der Praxis benötigt, die angeschafft und installiert werden müssen. Nähere Informationen finden sich unter: https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Fachanwendungen/gematik_VSD_Facharchitektur_VSDM_2_5_0.pdf.

Das Bundesgesundheitsministerium informierte zudem, dass „für die Zulassung von Komponenten und Diensten in der Telematikinfrastruktur (…) eine Sicherheitszertifizierung nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik gemäß dem Stand der Technik und der aktuellen Bedrohungslage (die regelmäßig zu überprüfen ist) erforderlich ist. Das zentrale Netz der Telematikinfrastruktur ist ein in sich geschlossenes Netz. Der Zugang zu diesem ist nur über sichere zentrale Zugangspunkte möglich.“ Die im Rahmen der Telematikinfrastruktur über eine VPN-Verbindung (virtuelles-privates-

Netz) versendeten Daten sind stets verschlüsselt. „Es ist für eine nicht im Besitz des Schlüssels befindliche Person mit den heute verfügbaren technischen Mitteln nicht möglich, nach den Standards der Telematikinfrastruktur verschlüsselte Daten zu entschlüsseln oder lesbar zu machen“, so das Bundesgesundheitsministerium.
Wichtig im Zusammenhang mit den weitgehenden Speichermöglichkeiten der eGK ist, dass diese **freiwillig** erfolgen. Versicherte müssen bei ihrem behandelnden Arzt, Therapeut oder Apotheker in die Speicherung ihrer Daten einwilligen. Möchten sie nicht, dass außer den Stammdaten (Name, Geburtsdatum, Adresse) sensible medizinische Daten auf der Karte gespeichert werden, müssen sie dem nicht zustimmen. Eine einmal erteilte Einwilligung kann jederzeit ohne Angaben von Gründen widerrufen werden. Hierüber sind die Patienten von ihrem Arzt und/oder der Krankenkasse aufzuklären.
Allerdings hat sich in diesem Bereich eine Sicherheitslücke gezeigt. Das digitale Gesundheitsnetzwerk soll eigentlich Ärzten und Kliniken den Zugriff auf elektronische Patientenakten ermöglichen. Doch auch IT-Experten des Chaos Computer Clubs konnten sich Zugang zum Netzwerk verschaffen, indem sie sich Arztausweise verschafften, die zur Authentisierung im System benutzt werden (siehe hierzu: https://www.mdr.de/nachrichten/politik/inland/sicherheitsluecke-digitales-gesundheitsdatennetz-100.html. Die Patientenakte ist von der reinen Gesundheitskarte zu unterscheiden. Bei der Patientenakte soll die gesamte Behandlung gespeichert werden. Dies ist momentan nicht der Fall, sodass aktuell noch keine Behandlungsdaten gespeichert wurden und daher keine Patientendaten in Gefahr waren. Nach dem Bekanntwerden der Sicherheitslücke im Gesundheitsnetzwerk stoppte die zuständige Gematik-Gesellschaft die Ausgabe von Praxis- und Arztausweisen. Außerdem wurden die Hersteller der Ausweise angewiesen, die betroffenen Identifizierungsverfahren für Arztausweise zu deaktivieren.

3.38 E-Mail für dich: aus Mexiko vom Klinikum

Cyber-Kriminelle nutzen für sogenannte Phishing-Mails (gefälschte E-Mails zur illegalen Beschaffung von persönlichen Daten) häufig die Kurzbezeichnungen von bekannten öffentlichen Einrichtungen, um

einen seriösen Eindruck zu erwecken. Der TLfDI empfiehlt, die Absenderadressen eingehender E-Mails genau zu prüfen, insbesondere, wenn die E-Mails Dateianhänge enthalten. Gerade ältere oder weniger aktuelle Mailprogramme erkennen Phishing-Mails nicht in jedem Falle.

Im Berichtszeitraum beschwerte sich der Inhaber einer Arztpraxis beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass er auf seinem Praxis-Mailaccount wiederholt Informationen seines Mailproviders (web.de) erhalten habe, mit dem Hinweis, dass für Mails aus einem Thüringer Klinikum „dringendster Verdacht auf Virenbefall“ bestünde. Die betreffenden Mails aus dem Klinikum wurden vom Mailprovider der Arztpraxis automatisch gelöscht. Der Beschwerdeführer hatte nach eigenen Angaben bereits mehrfach schriftlich und telefonisch den Geschäftsbereich Informationstechnologie des Klinikums kontaktiert, jedoch keine Antwort erhalten.
Daher wandte sich der Beschwerdeführer an den TLfDI und übersandte ihm die Hinweise seines Mailproviders. Bei dem Absender-Mailaccount, den der Provider als virenverseucht erkannt hatte, handelt es sich um folgende E-Mail-Adresse: Name.Vorname@med.xxxklinkum.demailto: und Namexxx@palme.com.mx.
In der E-Mail-Adresse des Klinikums waren Vor- und Nachname einer Mitarbeiterin des Klinikums vollständig angegeben. Die Empfängeradresse war die reguläre E-Mail-Adresse beim Mailprovider des ärztlichen Beschwerdeführers. Der Virenschutz des Mailproviders stufte die E-Mail vom Klinikum und deren Anhang als „gefährlich“ ein und löschte sie automatisch. Der Provider begründete die Löschung damit, dass der Absender-PC der E-Mail oder das Absender-Mobilgerät möglicherweise von einem Virus befallen sei.
Sowohl im Klinikum als auch in der betroffenen Arztpraxis werden besondere Kategorien von Daten – Gesundheitsdaten – gemäß Art. 9 Datenschutz-Grundverordnung (DS-GVO) in großem Umfang verarbeitet, die durch Schad- beziehungsweise Spam-Programme von unbefugten Dritten ausgespäht oder abgegriffen werden könnten. Daher wandte sich der TLfDI umgehend an das Klinikum und legte dar, dass der PC der betreffenden Mitarbeiterin des Klinikums möglicherweise mit Schadsoftware infiziert wurde und somit unter ihrem Namen Spam-Mails versendet werden könnten. Ebenso wäre es aus techni-

scher Sicht möglich, dass andere Mobilgeräte, die die Mitarbeiterin zur E-Mail-Versendung nutzt, ebenfalls Schadsoftware enthalten.
Der TLfDI forderte das Klinikum auf, den PC und die übrigen Mobilgeräte der Mitarbeiterin technisch zu überprüfen. Insbesondere sollte geklärt werden, ob tatsächlich E-Mails zu bestimmten Zeiten und Uhrzeiten von dem betreffenden Postfach des Klinikums an die E-Mail-Adresse des ärztlichen Beschwerdeführers verschickt wurden und ob der Inhalt dieser E-Mails rekonstruierbar ist. Auf Grundlage einer Rekonstruktion könnte festgestellt werden, ob die Mail tatsächlich Schadsoftware enthielt oder fälschlicherweise durch den Mailprovider des Beschwerdeführers als schädlich eingestuft wurde. Weiterhin sollte untersucht werden, ob ein Serversystem des Klinikums derartige E-Mails im Namen der Mitarbeiterin verschicken könnte. In diesem Fall wäre nicht der Arbeitsplatzrechner direkt betroffen, sondern es wäre das Serversystem selbst kompromittiert. Aus Datenschutzgründen empfahl der TLfDI dem Klinikum, bis zum Abschluss dieser Untersuchung von dem betreffenden PC keine E-Mails mehr zu versenden.
Die technische Überprüfung durch die IT-Abteilung und den IT-Sicherheitsbeauftragten des Klinikums ergab jedoch keinen Virenbefall bei Rechnern des Universitätsklinikums, das heißt, es wurden keine E-Mails mit den vom Beschwerdeführer genannten Absender- und Empfängeradressen über das zentrale Mailsystem des Klinikums versandt. Somit bestand im Klinikum auch keine Gefahr einer unbefugten Verbreitung oder eines unbefugten Zugriffs auf sensible Gesundheitsdaten von Patienten.
Offensichtlich hatten Cyber-Kriminelle Phishing-E-Mails versandt und hierfür auch gleichzeitig eine gefälschte Absenderadresse des Klinikums genutzt, um einen seriösen Eindruck zu erwecken. Dies ist eine häufige Form der digitalen Angriffe, die jedoch von den meisten aktuellen Mailsystemen zutreffend als Spam-Nachricht erkannt wird.
Der TLfDI übersandte dem Klinikum dennoch den E-Mail-Header für eine tiefgründige technische Prüfung im Interesse des erhöhten Schutzniveaus von Gesundheitsdaten. Der E-Mail-Header ist sozusagen der Briefumschlag der elektronischen Post. Er enthält Daten und Informationen über den Absender-Server, den Empfänger-Server, zwischengeschaltete Server, Sendezeiten der E-Mail, Absenderpostfach und Empfängerpostfach. Auch die weitergehende technische Überprüfung ergab keine Anhaltspunkte für einen Virenbefall von PCs oder Serversystemen im Klinikum. Jedoch teilte der IT-Sicher-

heitsbeauftragte des Klinikums mit, dass ihm bereits mehre vergleichbare Fälle mit gefälschten Absenderadressen des Klinikums für Phishing-Zwecke gemeldet wurden.
Konkret laufen diese Phishing-Attacken folgendermaßen ab: Vom Absender der Phishing-Mails wird ein zusätzlicher Name in die abgesendeten E-Mails eingefügt und der tatsächliche Sender steht in einer dreieckigen Klammer hinter dem eingefügten Namen. Im Falle des Beschwerdeführers stammte die Phishing-Mail von der Adresse Namexxx@palme.com.mx Die Domäne palme.com.mx führt zu einem in Mexico ansässigen Hoster. Hierzu ergab die Analyse folgende technische Informationen:

Domain der ausgehenden Mail:	palme.com.mx
Hostname:	mail.palm.com.mx
IP-Adresse:	xxx.xxx.xxx.xxxx
Netzwerkinhaber.	Telmex
Land / Staat:	Mexiko

Da das Klinikum auf derartige Vorfälle, das heißt, den Missbrauch gefälschter E-Mail-Adressen des Klinikums zu Phishing-Zwecken, und auf deren Urheber keinen Einfluss hat, lag in diesem Falle keine meldepflichtige Datenpanne nach Art. 33 DS-GVO vor. Das Klinikum teilte dem TLfDI aufgrund des Vorfalls mit, dass es im Hinblick auf die BSI Kritis-Verordnung „spezielle Maßnahmen zur Informations- und IT-Sicherheit etabliert und umgesetzt“ hat, um das erhöhte Datenschutzniveau von Gesundheitsdaten zu gewährleisten. Der TLfDI informierte den ärztlichen Beschwerdeführer über das Ergebnis der technischen Prüfung im Klinikum und forderte das Klinikum auf, sich auch selbst mit der Arztpraxis in Verbindung zu setzen, um die technischen Kommunikationswege besser abzusichern.

3.39 Informationspflicht nach Art. 13 und 14 DS-GVO

Mit Geltung der Datenschutz-Grundverordnung (DS-GVO) haben verantwortliche Stellen, die personenbezogene Daten verarbeiten, den betroffenen Personen bestimmte Informationen nach Art. 13 DS-GVO zur Datenverarbeitung mitzuteilen. So können betroffene Personen in die Lage versetzt werden, ihre Rechte angemessen auszuüben. Die In-

formationspflicht nach Art. 13 DS-GVO gilt für öffentliche (Kommunen und Behörden) sowie für nicht-öffentliche Stellen (Vereine, Unternehmen).

Eine Baustelle bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) ist die Erfüllung der Informationspflichten nach Art. 13 und 14 DS-GVO. Die DS-GVO regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei der betroffenen Person (Direkterhebung, Art. 13 DS-GVO) oder bei Dritten (Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Informationen verantwortlich ist. Auch der Verantwortliche, der die Daten direkt bei der betroffenen Person erhoben hat, kann über Art. 13 DS-GVO hinaus zur Mitteilung nach Art. 14 Abs. 3 Buchstabe c) DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem Empfänger offenbaren möchte. Bei der Direkterhebung sind (Art. 13 Abs. 1 DS-GVO) der betroffenen Person Informationen zur Verfügung zu stellen, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).
Mitzuteilen sind nach Absatz 1:

- Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls dessen Vertreter,
- Kontaktdaten des gegebenenfalls vorhandenen Datenschutzbeauftragten,
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung,
- wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe f) DS-GVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden,
- gegebenenfalls die Empfänger oder Kategorie von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

Zusätzlich sind nach Absatz 2 Informationen über

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder die Festlegung der Speicherdauer,

- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit),
- das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt,
- das Beschwerderecht bei der Aufsichtsbehörde

zur Verfügung zu stellen.

Bei der Dritterhebung unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und den zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Art. 14 Abs. 2 DS-GVO). Art und Inhalt der mitzuteilenden Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitgeteilt werden müssen. Allerdings hat die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt und somit auch keine Kenntnis darüber, welche personenbezogenen Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 Buchstabe d) DS-GVO verpflichtet, die Kategorien der verarbeitenden personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für die Betroffenen erkennbar wird, zu welchen Folgen die Verarbeitung führen kann. Nur dann kann er eine bewusste Entscheidung darüber treffen, ob er ergänzend von seinem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch machen sollte.

Bei der Dritterhebung ist zudem nach Art. 14 Abs. 2 Buchstabe f) DS-GVO die Datenquelle anzugeben und ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig festgestellt werden, muss dennoch eine allgemeine Information gegeben werden.

Bei der Dritterhebung ist weiterhin zu beachten, dass Angaben über die berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Buchstabe f) DS-GVO) nicht wie bei der Direkterhebung unter den Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 Buchstabe b) DS-GVO).

Der Zeitpunkt der Erfüllung der Informationspflichten

Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt beziehungsweise zur Verfügung gestellt werden. Bei der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemesse-

nen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den Umständen, darf aber einen Monat nicht überschreiten. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.
Nach Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in klarer und einfacher Sprache zu übermitteln.
Ein betroffener Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass im Schreiben vom Jugendamt keine Informationen nach Art. 13 DS-GVO angehängt wurden. Auf Nachfrage vom TLfDI hieß es, dass die erforderlichen Informationen dem Schreiben nicht angehängt wurden, da es von der zuständigen Mitarbeiterin in Vergessenheit geraten ist. Das Jugendamt versicherte, dass die Informationen nach Art. 13 DS-GVO immer versendet werden und es sich hierbei um ein Versehen handelte, sodass es bei einer Ermahnung geblieben ist. Ein Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 1 Buchstabe b) DS-GVO mit einer Geldbuße bestraft werden, allerdings nicht gegenüber öffentlichen Stellen.

Betroffene Personen können sich bei einer unterlassenen oder unvollständigen Information bei der zuständigen Aufsichtsbehörde nach Art. 77 DS-GVO beschweren. Die Erläuterungen zur Informationspflicht können Sie dem Kurzpapier Nr. 10 der Datenschutzkonferenz „Informationspflichten bei Dritt- und Direkterhebung“ entnehmen: https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_10_informationspflichten.pdf“

3.40 „Bankengeheimnis ade?“

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) befasste sich im Rahmen einer Anfrage eines Empfängers von Sozialleistungen mit der Frage, ob sich eine Sozial-

behörde bei der Bearbeitung des Leistungsantrages auch direkt an die Bank des Hilfebedürftigen wenden darf.

In welchen Fällen sich Sozialbehörden an Dritte, darunter Banken und Sparkassen, wenden dürfen, lässt sich wie folgt beantworten:
Immer dann, wenn eine Person einen Antrag auf staatliche Sozialleistungen stellt, sei es im Bereich Kranken- und Pflegeversicherung, Arbeitslosen- oder Rentenversicherung oder auch Wohngeld, ist die Bewilligung dieser Leistungen von unterschiedlichen Voraussetzungen abhängig. Der Leistungsträger, das heißt die Kranken- und Pflegeversicherung, aber auch das Jobcenter und Sozialamt, sind dabei darauf angewiesen, dass der Hilfebedürftige im Rahmen seiner Antragstellung die für die Bewilligung der Leistungen notwendigen Auskünfte erteilt und Belege vorlegt. Im Sozialrecht gilt dabei der sogenannte Grundsatz der vorrangigen Datenerhebung beim Betroffenen nach § 67a Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X). Das heißt, grundsätzlich muss der Betroffene die Daten mitteilen. Doch was passiert, wenn der Betroffene die Daten nicht mitteilt oder die Behörde bei der Bearbeitung des Antrages feststellt, dass der Hilfebedürftige möglicherweise Dinge verschweigt? Welche Befugnisse hat der Staat dann? Eine Möglichkeit ist die sofortige Versagung der Leistung. Eine andere Möglichkeit ist die Einholung von Auskünften bei Dritten. Der (deutsche) Gesetzgeber räumt dieses Auskunftsrecht den jeweiligen Sozialleistungsträgern nach § 60 Abs. 2 SGB II für die Grundsicherung für Arbeitssuchende und nach § 117 Abs. 3 SGB XII für die Sozialhilfe ein. In beiden Vorschriften werden Personen oder Stellen, die für den Leistungsbezieher Guthaben führen oder Vermögensgegenstände verwahren verpflichtet, „auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Aufgaben nach diesem Buch (im Einzelfall) erforderlich ist“. Diese Auskunftspflicht betrifft Arbeitgeber, unterhaltspflichtige Ehepartner, uneheliche Lebenspartner und auch Banken. Die Bank darf hierbei keine Kontoauszüge des Hilfebedürftigen vorlegen, da diese in der Regel auch Daten offenbaren, die für die Bearbeitung des Leistungsantrages nicht von Bedeutung sind. Allerdings sind Banken bei einem Auskunftsersuchen der Sozialbehörden verpflichtet, Auskunft über Anzahl der Konten, vorhandenes Guthaben oder verwahrte Vermögensgegenstände des Hilfebedürftigen zu erteilen. Die direkte Auskunft bei der Bank setzt dabei voraus, dass der Hilfebedürftige die Daten trotz Aufforderung

durch die Behörde nicht erteilt hat oder der Verdacht des Leistungsbetruges besteht. Für diese Fälle darf sich die Behörde direkt an die Bank wenden – im Übrigen ohne dies dem Hilfebedürftigen vorab mitteilen zu müssen (Art. 14 Abs. 5 l Buchstabe b) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 82a Abs. 1 Nr. 1 Buchstabe a SGB X). Erteilt der Hilfebedürftige hingegen die Auskünfte und gibt es auch sonst keine Anhaltspunkte für ein unlauteres Verhalten des Hilfebedürftigen, dürfen sich Sozialbehörden nur mit Zustimmung des Hilfebedürftigen an die Bank wenden.
Im Übrigen dürfen sich Sozialbehörden zur Vermeidung von Leistungsmissbrauch auch im Umfang begrenzte Informationen beim Zentralen Fahrzeugregister oder dem Melde- oder Ausländerzentralregister einholen, § 52a Abs. 1 SGB II.
Unabhängig von der Auskunftsverpflichtung Dritter dürfen die Jobcenter und Sozialämter einen sogenannten Kontenabruf unter den Voraussetzungen des § 93 Abs. 8 Abgabenordnung (AO) durchführen. Danach findet zwischen dem Bundeszentralamt für Steuern und den Sozialbehörden ein Datenabgleich über die Kontostammdaten von Hilfebedürftigen (beispielsweise Kontonummer, Tag der Kontoeinrichtung oder -auflösung, Name und Geburtsdatum des Inhabers sowie weiterer Verfügungsberechtigter) statt. Bevor ein solcher Datenabgleich durchgeführt werden darf, muss die Sozialbehörde jedoch versuchen, die Daten direkt von dem Hilfebedürftigen zu erlangen. Auch ist der Hilfebedürftige vor einem Datenabgleich von der Behörde hierüber zu informieren, was auch durch amtliche Vordrucke oder Merkblätter erfolgen kann, § 93 Abs. 9 AO.
Unabhängig davon, welche Stelle die Auskünfte gegenüber einer Sozialbehörde zu erteilen hat, gilt: Sozialbehörden dürfen nur über leistungserhebliche Tatsachen Auskünfte verlangen, die zur Bearbeitung des Antrages des Leistungsberechtigten *erforderlich* sind. Haben Hilfebedürftige Grund zur Annahme, dass Sozialbehörden zu Unrecht Daten – auch bei Dritten – erheben, sollten sie der Auskunft widersprechen (Art. 21 Abs. 1 DS-GVO).

3.41 Übermittlung von Steuerdaten: Ausland oder Zeitzone?

Städtenamen, die im Zusammenhang mit Zeitangaben in einer Lesebestätigung für E-Mails enthalten sind, stellen keine Orte dar, an denen eine versendete E-Mail gelesen wurde. Es handelt sich dabei le-

diglich um Angaben zu der betreffenden Zeitzone wie zum Beispiel die mitteleuropäische Zeit.

Durch das Online-Portal ELSTER (**EL**ektronische **ST**euer**ER**klärung) besteht bereits seit 1999 die Möglichkeit, dass die Kommunikation zwischen dem Bürger und der Finanzverwaltung auf elektronischem Weg erfolgen kann.
Mit der Bitte um Überprüfung der Rechtmäßigkeit einer Datenübermittlung durch das Online-Portal ELSTER wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Bürger hatte mehrfach versucht, sich ein ELSTER-Nutzerkonto anzulegen. Nachdem diese Versuche ohne Erfolg blieben, wandte sich der Beschwerdeführer mit einer E-Mail an die für Registrierungsprobleme bei ELSTER zuständige Stelle. Darin bat er um Rücksetzung seiner erfolglosen Registrierungsversuche. Aus einer entsprechenden Antwortmail (Lesebestätigung) der für die Registrierung zuständigen Stelle schloss der Bürger nun, dass einige seiner Steuerdaten von ELSTER in das Ausland übermittelt wurden. Zu dieser Auffassung gelangte der Beschwerdeführer, da die Nachricht neben dem Sende- und Lesezeitpunkt seiner E-Mail jeweils mehrere Städtenamen (Amsterdam, Berlin, Bern, Rom, Stockholm, Wien) enthielt.
Nach Durchsicht des geschilderten Falls konnte der TLfDI jedoch schnell für Aufklärung sorgen und dem Betroffenen mitteilen, dass die aufgeführten Städtenamen lediglich zu den in der E-Mail (Lesebestätigung) enthaltenen Zeitangaben gehörten. Diese markieren die sogenannte Zeitzone mitteleuropäische Zeit (MEZ). Die vom Beschwerdeführer vermutete unrechtmäßige Datenübermittlung durch ELSTER in das Ausland hatte also nicht stattgefunden. Ein Datenschutzverstoß lag nicht vor.

3.42 Können im Vorhinein angekreuzte Felder eine Einwilligung sein?

Eine wirksame Einwilligung nach Art. 4 Nr. 11 in Verbindung mit Art. 7 Datenschutz-Grundverordnung liegt nicht vor, wenn bereits im Vorfeld angekreuzte Felder nur zur Unterschrift vorgelegt werden.

Von Bankkunden wurden an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Beschwerden

darüber herangetragen, dass sie sich bei der Unterschrift zur „passgenauen Beratung“ getäuscht fühlten. Das Formular enthielt folgenden Passus, zu dem eingewilligt werden sollte:

„A. Analyse *der Daten zur Person*
Ich möchte individuell und möglichst passgenau beraten, betreut und über Produkte und Aktionen informiert werden.
Deshalb bin ich einverstanden, dass die Bank folgende Daten über mich verknüpft, gemeinsam auswertet und verwendet.“

Es folgen sodann Aufzählungen der verschiedenen Finanzprodukte, hierunter auch sehr heikle Punkte wie die Bonität, Einblick in Girokonten und die Einholung von Auskünften von „Verbundunternehmen“.
Die Verarbeitung dieser umfangreichen Auskünfte, die, wenn sie den Bereich der Bonität betreffen, besonders weitreichende wirtschaftliche Auswirkungen haben können, ist nur möglich, wenn eine Einwilligung nach Art. 4 Nr. 11 in Verbindung mit Art. 7 Datenschutzgrundverordnung (DS-GVO) vorliegt. Eine solche wird im Formular auch abgefragt, indem der Kunde ein entsprechendes Kreuz setzen muss. Bereits im Vorfeld angekreuzte Felder, die nur zur Unterschrift vorgelegt werden, gelten allerdings nicht als wirksame Einwilligung (siehe Erwägungsgrund 32 DS-GVO). Dem TLfDI wurde genau dies vorgetragen, dass nämlich die Formulare vorangekreuzt versandt werden. Auf Rückfrage äußerte das betroffene Kreditinstitut, dass die strikte Anweisung bestehe, dass die Formulare überhaupt nicht versandt werden dürfen. Die Einwilligung sei nur im Kundengespräch nach umfangreicher Erörterung einzuholen und zwar dann durch Setzen des entsprechenden Kreuzes. Einzelne Mitarbeiter, die hiergegen verstoßen würden, handelten weisungswidrig.
Der TLfDI wies darauf hin, dass dieses Verhalten durch Belehrung der Mitarbeiter abzustellen sei. In der Tat scheint sich ein Erfolg zu zeigen, da im Nachgang keine Meldungen dieser Art mehr eingegangen sind.

4. Fälle nicht-öffentlicher Bereich

© Praxis und Familie – Fotolia.

4.1 Datenschutzbeauftragter als IT-Sicherheitsbeauftragter – bestehen Interessenkonflikte?

Auch nach Inkrafttreten der Datenschutz-Grundverordnung gilt: Die Tätigkeiten eines IT-Sicherheitsbeauftragten und Datenschutzbeauftragten in Personalunion führen zu Interessenkonflikten und sind nicht miteinander vereinbar.

Im Berichtszeitraum wandte sich ein Mitarbeiter eines Unternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob es nach Inkrafttreten der europäischen Datenschutz-Grundverordnung (DS-GVO) möglich sei, die Tätigkeiten des IT-Sicherheitsbeauftragten und des Datenschutzbeauftragten in Personalunion auszuführen.
Für die Entscheidung, eine Person beide Aufgaben übernehmen zu lassen, spreche die hohe Arbeitsbelastung, das knappe Personal und

die Tatsache, dass in beiden Funktionen sehr gute IT-Kenntnisse notwendig seien. Der in Frage kommende Mitarbeiter fungierte in dem Unternehmen zudem als IT-Administrator und sei sich, nach eigenem Bekunden, der Interessenkonflikte bewusst und versuche die Aufgabenbereiche zu trennen.
Bereits zur alten Rechtslage vertrat der TLfDI im 3. Tätigkeitsbericht zum nicht-öffentlichen Bereich (Beitrag 2.3) die Auffassung, dass in dieser Konstellation Interessenkonflikte drohen und daher die Bestellung zum betrieblichen Datenschutzbeauftragten (bDSB) unzulässig sei.
Auch nach neuem Recht hat der TLfDI grundsätzliche Bedenken hinsichtlich der Bestellung zum IT-Sicherheitsbeauftragten und Datenschutzbeauftragten in Personalunion.
Nach Art. 37 Abs. 5 DS-GVO wird der Datenschutzbeauftragte aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die Aufgaben des Datenschutzbeauftragten zu erfüllen, benannt. Nach Art. 38 Abs. 6 DS-GVO ist es grundsätzlich möglich, dass der Datenschutzbeauftragte auch andere Aufgaben übernehmen kann. Dabei muss allerdings zwingend sichergestellt werden, dass es nicht zu Interessenkonflikten kommt. Interessenkonflikte sind immer dann anzunehmen, wenn der Datenschutzbeauftragte sich selbst (im Rahmen seiner anderweitigen Tätigkeit) kontrollieren müsste, oder die Unabhängigkeit des Datenschutzbeauftragten gefährdet wäre. Für eine Vereinbarkeit der Tätigkeiten des IT-Sicherheitsbeauftragten und Datenschutzbeauftragten spricht zunächst, dass ein umfassendes Wissen im Bereich der IT und IT-Sicherheit für Beurteilungen des bDSB hilfreich ist. Der bDSB muss auch an der Erstellung eines IT-Sicherheitskonzeptes mitarbeiten.
Während die Tätigkeit des bDSB auf die Gewährleistung der Betroffenenrechte ausgerichtet ist, sind die Aufgaben des IT-Sicherheitsbeauftragten auf die Gewährleistung der Informationssicherheit des Unternehmens ausgerichtet. Dies führt dazu, dass der IT-Sicherheitsbeauftragte im Rahmen der Gefahrenabwehr von Angriffen Dritter auf IT-Systeme des Unternehmens oftmals an einer umfangreichen Sammlung personenbezogener Daten interessiert ist, um Missbrauch zu entdecken, während der dDSB unter Berücksichtigung der Schutzziele der DS-GVO eine Begrenzung der Sammlung personenbezogener Daten anstrebt. Auch mit Blick auf die Speicherdauer personenbezogener Daten vertreten IT-Sicherheitsbeauftragte und Datenschutzbeauf-

tragte häufig unterschiedliche Positionen. Während der Datenschutzbeauftragte aus Gründen der Datensparsamkeit für eine kurze Speicherdauer ist, strebt der IT-Sicherheitsbeauftragte zu Zwecken der Störungserkennung und -analyse eine möglichst langfristige Speicherung der Daten an. Auch ist es im Interesse des IT-Sicherheitsbeauftragten, mit Audit-Logs herauszufinden, welche Personen (intern oder extern) welche Aktionen auf welchen Systemen durchführen, um Schwachstellen herauszufinden. Dies widerspricht der Aufgabe des Datenschutzbeauftragten, der möglichst wenig Überwachung der Mitarbeiter anstrebt. Zudem bestehen hinsichtlich der weiteren Funktion als IT-Administrator Interessenkonflikte, da der Mitarbeiter insoweit weisungsgebunden in die Struktur der IT eingebunden ist und sich in seiner Funktion als Datenschutzbeauftragter selbst kontrollieren müsse.
Der Anfragende wurde darauf hingewiesen, dass der TLfDI die Bestellung eines Datenschutzbeauftragten als von Anfang an unwirksam ansieht, da ein Interessenkonflikt vorlag.

4.2 Anwaltswerbung mit Daten Dritter

Wenn ein Rechtsanwalt Akten einsieht, nimmt er notwendigerweise auch Daten von Personen zur Kenntnis, die nicht seine Mandanten sind. Diese Daten dürfen ohne Einwilligung der betroffenen Person nicht zu Zwecken der Werbung verwendet werden, da keine Rechtsgrundlage aus Art. 6 Abs. 1 Datenschutz-Grundverordnung existiert.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag im Berichtszeitraum folgender Sachverhalt im Rahmen von mehreren Beschwerden zur Überprüfung vor: Eine Rechtsanwaltskanzlei erhob durch Akteneinsichten in mehreren laufenden Großinsolvenzverfahren Gläubigerdaten. Diese personenbezogenen Daten wurden sodann zunächst an einen Verein übermittelt, welcher durch den Inhaber der Kanzlei gegründet wurde. Über den Verein wurden Schreiben an die einzelnen Gläubiger versandt. Darin wurde um den Beitritt in eine Interessengemeinschaft gebeten, die die Interessen der Gläubiger zur Sicherung ihrer Ansprüche bündeln wollte. Dem Schreiben war ein entsprechender Antwortbogen beigefügt. Den Gläubigern wurde angekündigt, dass sie ein Informationsanschreiben hinsichtlich möglicher rechtliche Ansprüche gegenüber den insolventen Gesellschaften oder den Gesellschaftern erhalten

würden, sobald sie diesen Antwortbogen zurücksenden würden. Dem Informationsschreiben war dann zumeist eine Vollmachtsurkunde beigefügt und es wurde auf die Gebührenhöhe hingewiesen. Es wurde hier auch eine Frist zur Übersendung der entsprechenden Beauftragung gesetzt. Als Zweck der Datenerhebung stand daher keine Interessenbündelung bereits bestehender Mandate im Vordergrund, sondern die werbliche Ansprache zur Akquirierung weiterer Mandate für die Kanzlei. Auch der gegründete Verein diente allein diesem Zweck. Der TLfDI sieht die hier erfolgte Erhebung der Daten zum Zweck der Übermittlung an den Verein, die Übermittlung selbst und die Nutzung der personenbezogenen Daten als nicht rechtmäßig an. Die werbliche Ansprache der nicht durch die Kanzlei mandatierten Gläubiger kann auf keine Rechtsgrundlage gestützt werden. Die Verarbeitung von personenbezogenen Daten muss nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) rechtmäßig erfolgen. Eine rechtmäßige Datenverarbeitung ergibt sich aus den Voraussetzungen des Art. 6 Abs. 1 DS-GVO. Zunächst erfolgte die Übermittlung der personenbezogenen Daten an den gegründeten Verein zum Zweck der werblichen Ansprache unrechtmäßig. Eine Einwilligung der nichtmandatierten Gläubiger in die Übermittlung der Daten lag nicht vor. Auch auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO kann die Übermittlung nicht gestützt werden. Danach ist die Verarbeitung rechtmäßig, soweit sie zur Wahrnehmung berechtigter Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Im Rahmen der Interessenabwägung ist eine einzelfallorientierte Abwägung im Hinblick auf die Interessen des Verantwortlichen als auch der betroffenen Personen vorzunehmen. Hierbei sind nach Erwägungsgrund 47 die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen. Daneben ist aber auch zu fragen, was objektiv vernünftigerweise erwartet werden kann und darf. Die Kanzlei verfolgte durch die Übermittlung der Daten werbliche Zwecke, da der Verein den Gläubigern die Beratung der eigenen Vertrauensanwälte, also die betreffende Rechtsanwaltskanzlei, empfohlen hatte. Dies stellt zwar ein berechtigtes Interesse des Verantwortlichen dar, jedoch konnten die betroffenen Gläubiger nicht erwarten, dass deren Adressen, welche aus einem Akteneinsichtsrecht stammen, von einem Rechtsanwalt

an einem Verein für dessen Werbezwecke weitergegeben werden. Von einem Organ der Rechtspflege wird erwartet, dass personenbezogene Daten außerhalb der geltenden Bestimmungen insoweit nicht verarbeitet werden. Zudem handelte es sich um eine sehr hohe Anzahl von Personen, welche von der Übermittlung betroffen waren. Daher geht der TLfDI von einem Überwiegen der Interessen der betroffenen Gläubiger aus.
Auch die Nutzung der Gläubigerdaten zu werblichen Zwecken kann auf keine geltende Rechtsgrundlage gestützt werden. Auch hier bliebe allenfalls Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO (siehe oben). Im vorliegenden Fall überwiegen jedoch die Interessen der betroffenen Personen. Hinsichtlich der Interessenabwägung gilt bereits das vorher Gesagte. Zudem ist die Werbung eines Rechtsanwalts nach § 43b Bundesrechtsanwaltsordnung nur erlaubt, soweit sie über die berufliche Tätigkeit in Form und Inhalt unterrichtet und nicht auf die Erteilung eines Auftrags im Einzelfall gerichtet ist. Durch die Übersendung des konkreten Angebots zur Übernahme des Mandates mit Verweis auf die Gebühren nach dem Rechtsanwaltsvergütungsgesetz sowie die Fristsetzung hinsichtlich der Mandatserteilung beziehungsweise Rücksendung der Vollmachtsurkunde liegt ein Verstoß gegen diese Vorschrift vor. Insbesondere wird durch die Formulierungen die Wahlfreiheit des noch nicht mandatierten Gläubigers eingeschränkt und dieser bedrängt beziehungsweise in seiner Entscheidungsfreiheit überrumpelt. Auch diese Umstände führen letztendlich dazu, dass die Interessen der nicht-mandatierten Gläubiger überwiegen.
Der TLfDI hat die betreffende Rechtsanwaltskanzlei angehört und hier ein Verbot nach Art. 58 Abs. 2 Buchstabe f) DS-GVO hinsichtlich der werblichen Nutzung von Gläubigeradressen aus Insolvenzakteneinsichten sowie der Weitergabe der Daten an andere Empfänger zur Wahrnehmung des gleichen Zwecks erlassen.

4.3 Datenschleuder im Internetportal für Immobilien

Mieterdaten dürfen zum Zweck eines Immobilienverkaufs nicht verarbeitet werden. Soweit sich potenzielle Käufer über die Jahresmieteinnahmen und den jeweiligen Mietzins informieren wollen, kann eine anonymisierte Mieterliste eingesehen werden.

In einem Internetportal für Immobilien wurde ein Mehrfamilienhaus zum Verkauf angeboten. Eines der dort inserierten Bilder zeigte eine

detaillierte Übersicht über die vermieteten Wohnungen und Mieteinnahmen nebst den Namen der Mieter. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr von dieser Datenschleuder durch einen aufmerksamen Bürger. Dieser war selbst nicht von der Datenverarbeitung betroffen.
Im Laufe des Verfahrens stellte sich heraus, dass das Immobilienmaklerbüro mit dem Eigentümer des Mehrfamilienhauses einen Makler- und Betreuungsvertrag (Verkaufsauftrag) zum Verkauf der Immobilie als Kapitalanlage geschlossen hatte. Hierfür hatte der Verantwortliche verschiedene Fotos der Immobilie aufgenommen und Informationen vom Eigentümer für die Erstellung eines Verkaufsexposés erhalten. Die Informationen des Eigentümers zur Immobilie und der Mietverhältnisse werden regelmäßig in anonymisierten und nicht-anonymisierten Mieterlisten zusammengestellt. Die nicht-anonyme Mieterliste wurde für interne Zwecke verwendet und enthielt Angaben zum Namen und der Wohnung der Mieter, zum Mietbeginn und zur Jahresmiete. Die anonymisierte Mieterliste wurde zum Beispiel Kaufinteressenten zugesandt, die sich zunächst über die Jahresmieteinnahmen und den jeweiligen Mietzins informieren wollten und gegebenenfalls eine Vorabanfrage bei dem finanzierenden Kreditinstitut zu stellen beabsichtigten.
Die Mieterliste und die zur Verfügung gestellten Informationen zum betreffenden Mehrfamilienhaus wurden von einem Mitarbeiter versehentlich in nicht-anonymisierter Form in dem Ordner gespeichert, der für die Veröffentlichung in dem Internetportal genutzt wurde. So kam es zur Veröffentlichung der Mieterdaten. In der veröffentlichten Mieterliste waren folgende personenbezogene Mieterdaten enthalten:

- Vor- und Nachname,
- Adresse,
- Höhe des monatlichen Mietzinses,
- Etage und Quadratmeteranzahl der Wohnung.

Damit wurden personenbezogene Mieterdaten verarbeitet, was nur rechtmäßig ist, wenn nach Art. 6 Abs. 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO) die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist. Zwar mag dem Immobilienmaklerbüro ein Mietvertrag mit den betroffenen Mietern vorliegen, zur Erfüllung dessen ist jedoch eine Veröffentlichung der Mieterdaten an eine unbestimmte Anzahl Dritter nicht erforderlich. Vielmehr dient der Mietvertrag der Vermietung von Wohnraum und der Zahlung des darin festgelegten Mietbetrages. Weiterhin kann die Verarbeitung der

Mieterdaten rechtmäßig sein, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist, Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Allerdings nur, soweit nicht die Interessen oder Grundrechte und Grundfreiheiten der Mieter entgegenstehen. Das Interesse des Verantwortlichen begründet sich in dem Verkauf des Mehrfamilienhauses. Hierzu ist es nicht erforderlich, die Mieterdaten zu veröffentlichen. Die schutzwürdigen Interessen der betroffenen Mieter stehen dieser Veröffentlichung entgegen, denn die Frage, welche Wohnung ich bewohne und wieviel Miete ich dafür zahle, gehört zum privaten Lebensbereich einer Person. Auch eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO lag für die hier erfolgte Datenverarbeitung nicht vor.
Das Immobilienmaklerbüro hat unmittelbar nach Kenntniserlangung dieses Vorfalls die Mieterliste aus dem Exposé zum Mehrfamilienhaus und dem System gelöscht. Darüber hinaus wurde der Cache (Pufferspeicher zu einem Hintergrundmedium der Webseite) zur Mieterliste unwiderruflich beim Betreiber des Internetportals gelöscht, damit der Inhalt der Datei physisch nicht mehr auffindbar ist und auch nicht wiederhergestellt werden kann. Weiterhin haben die Mitarbeiter zusätzlich zur Verpflichtung auf das Datengeheimnis eine Schulung zum Datenschutz nach der DS-GVO absolviert. Die Mieter wurden über die Veröffentlichung der Mieterliste informiert und das Immobilienmaklerbüro hat sich zu diesem Vorfall bei den betroffenen Mietern entschuldigt. Darüber hinaus wurde gegen das Immobilienmaklerbüro ein Bußgeldverfahren eingeleitet.

4.4 Datenverarbeitung im Rahmen einer Wohnungseigentümergemeinschaft

Nach dem Grundsatz der Zweckbindung und der Datensparsamkeit dürfen nicht alle personenbezogenen Daten verarbeitet werden, die der Eigentümer dem Verwalter einer Wohnungseigentümergemeinschaft preisgibt. Insbesondere vor einer zulässigen Übermittlung der personenbezogenen Eigentümerdaten an Dritte ist eine Prüfung vorzunehmen, welche Daten für welche Zwecke verarbeitet werden dürfen.

Ein Beschwerdeführer wollte im Berichtszeitraum vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wissen, ob es rechtmäßig ist, einen Brief an alle Miteigentü-

mer einer Wohnungseigentümergemeinschaft (WEG) zu übermitteln. Ein Eigentümer hat den Verwalter der WEG in einem Brief über den Eigentümerwechsel seiner Wohnung informiert. Dieser Brief wurde allen Miteigentümern als Anlage zu der Beschlussvorlage vom Verwalter der WEG übermittelt. In diesem Brief waren die personenbezogenen Daten des Eigentümers zur neuen Wohnanschrift, zum Wohnungsverkauf sowie zum Kreditinstitut enthalten.

Zu prüfen war, ob der Verwalter diese personenbezogenen Daten zu Recht an die anderen Eigentümer übermittelt hat. Artikel 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) regelt den Begriff des Verantwortlichen. Darin wird festgelegt, dass 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, Verantwortlicher ist. Das bedeutet, dass der Verwalter Verantwortlicher für die Übermittlung der personenbezogenen Eigentümerdaten ist. Hierfür bedarf es einer Rechtsgrundlage aus Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO. Danach ist die Verarbeitung personenbezogener Daten erlaubt, wenn

a) eine Einwilligung der Betroffenen vorliegt,
b) die Daten zur Erfüllung oder Durchführung eines Vertrages erforderlich sind oder
f) die Daten zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sind, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.

Eine Einwilligung des Beschwerdeführers nach Art. 6 Abs. 1 Satz 1 Buchstabe 1) DS-GVO zur Übermittlung seiner Adress- und Bankdaten und seiner Daten zum Wohnungsverkauf an die übrigen Miteigentümer lag dem Verwalter der WEG nicht vor. Da sich die Erfordernisse nach einem Eigentümerwechsel aus dem Wohnungseigentumsgesetz (WEG) ergeben, kommt die Erfüllung eines Vertrags als Erlaubnistatbestand nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ebenfalls nicht in Betracht. Es kommt daher darauf an, ob die Übermittlung zur Wahrung der berechtigten Interessen des Verwalters erforderlich gewesen ist und nicht die Interessen der betroffenen Person überwiegen.

Zur Abwicklung des Eigentümerwechsels ist es nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO erforderlich gewesen, dem Verwalter

der WEG, die in dem Schreiben zu dem Eigentümer enthaltenen Angaben zu machen.
Da mit dem Ausscheiden eines Eigentümers der Verwalterbeirat nach § 29 WEG aufgefüllt werden sollte, ist es ebenfalls erforderlich gewesen, die verbleibenden Eigentümer darüber zu informieren.
Im Ergebnis war es nach Auffassung des TLfDI jedoch nicht erforderlich und daher auch nicht rechtmäßig, den handschriftlichen Brief des Eigentümers allen Eigentümern der WEG in Gänze zu übermitteln. Die bloße Information zum Eigentümerwechsel und der damit verbundenen Notwendigkeit der Ergänzung des Verwalterbeirats wäre zur Zweckerreichung angemessen und ausreichend gewesen.
Dies gilt auch, wenn der Verwalter der WEG vorträgt, die Bank- und Abrechnungsdaten für eventuelle mit der Jahresabrechnung anfallende Rückforderungen zu benötigen. Kommt es im Laufe der Wirtschaftsperiode zu einem Eigentümerwechsel, so schuldet der veräußernde Wohnungseigentümer das nach Wirtschaftsplan zu zahlende Hausgeld bis zum Eigentümerwechsel. Ab diesem Zeitpunkt hat dann der Erwerber die Hausgelder nach dem Wirtschaftsplan zu zahlen. Wird die Jahresabrechnung der letzten Wirtschaftsperiode vor dem Eigentümerwechsel beschlossen, so stehen die Abrechnungsguthaben dem Veräußerer zu, etwaige Fehlbeträge hat er nachzuzahlen. Der Eigentümer hatte seine Zahlungsverpflichtungen nach dem Wirtschaftsplan vor der Veräußerung des Wohneigentums noch nicht erfüllt. In diesem Fall kann die Gemeinschaft gegen den Eigentümer Zahlungsansprüche auch nach seinem Ausscheiden geltend machen. Da dies durch den Verwalter geschieht, war die Übermittlung der Bankdaten an alle Miteigentümer für die Geltendmachung etwaiger Zahlungsansprüche nicht erforderlich. Letztlich wurde gegen den Verwalter der WEG ein Bußgeldverfahren eingeleitet. Eine abschließende Entscheidung im Bußgeldverfahren bleibt abzuwarten.

4.5 Gefrorener Datenschutz – Eiscafé totalüberwacht

Eine Videoüberwachung von Cafétischen sowie Sitzbereichen der Gäste ist unzulässig. Hier unterhalten sich die Gäste, essen und trinken zusammen. Dieses Verhalten ist auch nach der Rechtsprechung (vergleiche AG Hamburg, Urteil vom 22. April 2008, Az.: 4 C 134/08) dem Freizeitbereich zuzuordnen. Ein Eingriff in die Persönlichkeitsrechte in diesen Bereichen wiegt besonders schwer, da die unbeein-

trächtigte Kommunikation gestört wird und ein unbeobachteter Aufenthalt im Cafébereich nicht möglich ist.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde, dass in einem Eiscafé unter anderem die Mitarbeiter beim Ausgeben des Eises sowie die Gäste im kompletten Cafébereich mittels mehrerer Kameras überwacht würden. Der TLfDI wandte sich daher zunächst mit einem umfassenden Auskunftsersuchen an den Betreiber des Eiscafés. Dieser beantwortete das Auskunftsersuchen vollumfänglich. Allein in dem überschaubaren Café wurden seitens des Verantwortlichen vier Videokameras betrieben. Zwei der dort angebrachten Kameras waren auf den Zugang zur Außenterrasse sowie auf die Cafétische und Sitzbereiche der Gäste ausgerichtet. Bei Tageslicht wurde auch die direkt an dem Café befindliche Außengastronomie abgebildet. Die übrigen Kameras betrafen den Bereich hinter der Verkaufstheke.
Die Beurteilung der Zulässigkeit einer Videoüberwachung erfolgt auf Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO). 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 überwiegen, die den Schutz personenbezogener Daten erfordern.
Ein berechtigtes Interesse kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Als Zweck für die Kameras im Cafébereich wurde seitens des Verantwortlichen angegeben, dass diese angebracht wurden, um Zechprellerei entgegenzuwirken. Zudem sei in der Vergangenheit nachts die Terassenbestuhlung entwendet worden. Auch sei in der Vergangenheit bereits die Situation eingetreten, dass Mitarbeiter Waren an Kunden kostenlos gereicht hatten oder Wechselgeld absichtlich falsch herausgegeben wurde.
Sofern die Videoüberwachung zur Gefahrenabwehr dient, zum Beispiel um vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, muss seitens des Verantwortlichen eine konkrete Gefahrenlage nachgewiesen werden. Dies kann durch Nennung von Beschädigungen, besonderen Vorfällen in der Vergangenheit (Datum, Höhe des Schadens, Ereignis) oder durch Nennung von polizeilichen Tagebuchnummern beziehungsweise staatsanwaltschaftlichen Aktenzeichen erfolgen. Die

einfache pauschale Benennung von Ereignissen in der Vergangenheit reicht nicht aus, da eine aktuelle Gefahrenlage gegeben sein muss.
Darüber hinaus muss die Videoüberwachung für den genannten Zweck erforderlich sein. Das heißt, die Videoüberwachung muss für den genannten Zweck geeignet sein und es darf kein anderes gleich wirksames Mittel zur Verfügung stehen, welches weniger in die Rechte der betroffenen Personen eingreift.
Hier bestanden bereits Bedenken hinsichtlich der Geeignetheit der Kameras aufzudecken, ob seitens der Mitarbeiter Wechselgeld absichtlich falsch herausgegeben wurde. In den Ess- und Aufenthaltsbereichen besteht zudem während den Öffnungszeiten keine hohe Gefahr für das Eigentum der Gastronomen. Ferner ist im Inneren des Cafébereichs selten mit Delikten wie Zechprellerei zu rechnen, da durch die Anwesenheit des Personals und der anderen Gäste eine soziale Kontrolle erfolgt. Die Hemmschwelle für eine strafbare Handlung gegen den Gastronomen ist daher sehr hoch. Die Gefahr würde eher im Außenbereich bestehen, aber auch hier ist durch die Anwesenheit der anderen Gäste und durch mögliche bauliche Maßnahmen die Gefahr eher gering. Zudem kann das anwesende Personal im Notfall eingreifen oder die Polizei verständigen. Hinsichtlich des Diebstahls der Terassenbestuhlung können ebenfalls zunächst mildere Maßnahmen ergriffen werden, zum Beispiel ist es möglich, die Stühle und Tische so aneinander zu ketten, dass ein Diebstahl erheblich erschwert wird. Erst wenn andere Maßnahmen überhaupt nicht greifen, könnte eine – temporäre – Videoüberwachung eingesetzt werden.
Neben dem „Ob“ des Einsatzes der Videotechnik ist auch das „Wie“ Gegenstand der Erforderlichkeitsprüfung. Insbesondere beim nächtlichen Diebstahl der Terassenbestuhlung wäre eine Überwachung außerhalb der Geschäftszeiten des Cafés ausreichend. Aber auch erst dann, wenn alle anderen Maßnahmen erfolglos geblieben sind.
Weiterhin ist im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO eine einzelfallorientierte Interessenabwägung durchzuführen, 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 Interessen, Grundrechte und Grundfreiheiten eingreift und welche möglichen Folgen für Betroffene daraus re-

sultieren können. Ob vernünftige Erwartungen bestehen, beurteilt sich danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert ist oder eventuell wegen eines Beziehungszusammenhangs sogar verlangt wird oder nicht.
In den Sitzbereichen und der Außengastronomie halten sich die Gäste typischerweise über längere Zeit auf, hier essen sie, trinken und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu (vergleiche AG Hamburg, Urteil vom 22. April 2008, Az.: 4 C 134/08). Ein Eingriff in die Persönlichkeitsrechte in diesen Bereichen wiegt daher besonders schwer. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt im Cafébereich. Die betroffenen Personen erwarten gerade in diesen Bereichen nicht, überwacht zu werden. Daher überwiegen hier die Interessen der von der Videoüberwachung erfassten Gäste in diesen Bereichen die hier bereits nicht nachgewiesenen berechtigten Interessen des Gastronomen.
Die betriebene Videoüberwachung des Verantwortlichen war daher in diesen Bereichen unzulässig und die Kameras, welche diese Bereiche überwachten, waren abzuschalten beziehungsweise abzubauen. Eine entsprechende Anordnung wurde seitens des TLfDI getroffen.

4.6 Die Tücken bei Bewerbungen per E-Mail

Sollen Bewerbungen auf ausgeschriebene Stellen per E-Mail erfolgen, sind die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Bewerberdaten gegen unbefugte Kenntnis zu treffen. Dies gilt auch für Eingangsbestätigungen per E-Mail.

Ein Bewerber um eine Anstellung bei einer Landeseinrichtung beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil dort offenbar noch Daten aus früheren erfolglosen Bewerbungen vorhanden waren, die aus seiner Sicht längst hätten gelöscht sein müssen. Seine aktuelle Bewerbung per E-Mail hatte er unter Nutzung einer erst seit Kurzem eingerichteten E-Mail-Adresse übersandt. Die Eingangsbestätigung ging allerdings an eine alte E-Mail-Adresse. Daraus zog die betroffene Person den Schluss, dass man in der Stelle offenbar alte Bewerbungen vorhielt. Auf Anfrage beim Verantwortlichen, wie es dazu kommen konnte und wie die aus datenschutzrechtlicher Sicht nicht unproblematische Bewerbung generell geregelt sei, teilte dieser dem TLfDI

mit, man lösche Bewerberdaten selbstverständlich entsprechend der definierten Löschfristen zeitnah. Der konkrete Sachverhalt zu der in Rede stehenden Bewerbung könne aus diesem Grund nicht rekonstruiert werden. Zur Reglementierung datenschutzrechtlicher Fragestellungen sei ein Datenschutzhandbuch im Einsatz, das auch die Anforderungen an die Datenverarbeitung im Rahmen von Bewerbungsverfahren regele. Die Bewerber könnten die Bewerbung verschlüsselt übersenden. Durch ein mehrstufiges System von Zugriffsrechten sei ein unbefugter Zugriff intern ausgeschlossen. Die Aufnahme in das interne Bewerbermanagementsystem und der Zugriff auf dieses System sei nur für autorisierte Personen zugelassen. Bewerbungsunterlagen dürften nur den Personen zur Verfügung gestellt werden, die an der Personalauswahl beteiligt sind.
Eine Rückantwort an eine „alte“ E-Mail-Adresse konnte sich die verantwortliche Stelle nur vor dem Hintergrund der Autofill-Funktion des Posteingangs-Programms erklären, indem das Programm zumindest Teile der eingegebenen Adresse erkannte und sofort automatisch vervollständigte, und nahm die Anfrage zum Anlass, Strategien zur Vermeidung eben dieser Funktion zu entwickeln. Der TLfDI hatte keine Bedenken zum geschilderten Umgang mit den Bewerberunterlagen und wies darauf hin, dass bis zu einem Ausschluss der Autofill-Funktion bei der Versendung von Nachrichten an die Bewerber besonderes Augenmerk auf die Aktualität beziehungsweise Richtigkeit der übernommenen E-Mail-Adresse zu richten ist.
Der TLfDI unterrichtete die betroffene Person über die Feststellungen und dass im Hinblick auf die Autofill-Funktion geeignete Maßnahmen seitens des Verantwortlichen eingeleitet wurden. Eine weitergehende Prüfung des Einzelfalls durch den TLfDI konnte allerdings nicht erfolgen, da die betroffene Person Anonymität wünschte.
Die Problematik von Bewerbungen per E-Mail war bereits mehrfach Gegenstand datenschutzrechtlicher Prüfungen. (vergleiche Punkt 6.10 des 11. Tätigkeitberichts des TLfDI). Ein Verantwortlicher darf nur dann zur Bewerbung per E-Mail auffordern, wenn die technischen und organisatorischen Maßnahmen zum Schutz der Bewerberdaten gegen unbefugte Kenntnis getroffen sind. Wird den Bewerbern die Übersendung der Bewerbung in verschlüsselter Form ermöglicht, was aufgrund der Sensibilität der Bewerbungsdaten angemessen ist, sind umgekehrt auch Reaktionen der verantwortlichen Stelle auf Bewerbungen gegen unbefugte Kenntnis auf dem Transport besonders zu sichern. Dies bedeutet, dass, wenn eine Eingangsbestätigung nicht ver-

schlüsselt wird, weder aus dem Header noch aus dem Inhalt für Unbefugte erkennbar sein darf, dass es sich um die Bestätigung einer Bewerbung handelt. In einem solchen Fall dürfte nur neutral der „Eingang eines Schreibens vom …(Datum)“ bestätigt werden. Hierauf wurde der Verantwortliche nochmals hingewiesen.

4.7 Einwilligung im Postkartenformat

Eine Einwilligungserklärung muss freiwillig abgegeben werden und über eine klare Textgestaltung und leichte Sprache verfügen. Ebenso wichtig ist die Zweckdarstellung der Einwilligungserklärung. Eine Belehrung über den Widerruf und die Folgen der Verweigerung der Einwilligung müssen ebenfalls enthalten sein. Die Einwilligungserklärung darf auch nicht an weitere Dienstleistungen gekoppelt sein (Kopplungsverbot), Art. 7 Datenschutz-Grundverordnung.

Ein Energieversorger übersandte seinen Kunden eine Einwilligungserklärung für Werbe- und Marktforschungszwecke. Der Energieversorger bat um Rücksendung dieser Einwilligung per Postkarte. Darauf befanden sich Name, Kontaktdaten und Geschäftspartner-Nummer der von der Datenverarbeitung betroffenen Personen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sieht in dem Versand der Postkarte und den darauf enthaltenen personenbezogenen Daten eine Datenverarbeitung in Form der Datenübermittlung, wofür keine gesetzliche Grundlage gegeben ist. Der Energieversorger wurde darauf hingewiesen, dass die Einholung der Einwilligungserklärung für oben genannte Zwecke jedenfalls gesetzeskonform organisiert werden und die Zuleitung der Einwilligungserklärung in der Art und Weise erfolgen muss, dass die darin enthaltenen personenbezogenen Daten nicht an Dritte übermittelt werden. Der TLfDI stellte weiterhin fest, dass die Einwilligungserklärung für Werbe- und Markforschungszwecke nicht den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an eine wirksame Einwilligung entsprach. Die Artikel-29-Datenschutzgruppe hat die Anforderungen an eine wirksame Einwilligung gemäß DS-GVO in der Leitlinie WP 259 niedergeschrieben (https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html).

Im Ergebnis bedurfte es der Nachbesserung im Hinblick auf die Freiwilligkeit, die Textgestaltung und Sprache, die Zweckdarstellung der Einwilligung, den Widerruf sowie die Folgen der Verweigerung. Aus der Karte ließ sich nicht eindeutig entnehmen, dass die Erteilung der Einwilligung und der Rückversand freiwillig waren. Es fehlte der Hinweis, dass die Einwilligung jederzeit für die einzelnen Kontaktwege **und** -zwecke mit Wirkung für die Zukunft widerrufen werden kann. Auf die Folgen der Verweigerung der Einwilligung war nicht hingewiesen worden. Die Kunden konnten in Form des Ankreuzens zwischen den Kontaktwegen

- ☐ E-Mail
- ☐ Telefon und Fax

auswählen. Hierfür war die Angabe der E-Mail-Adresse, Telefon- oder Faxnummer vorgesehen.

Der Energieversorger argumentierte, in dem Rückversand der ausgefüllten Postkarte an ihn sei keine Datenübermittlung zu sehen und begründete dies mit dem Postgeheimnis. Sobald der Kunde die Postkarte ausgefüllt hat, übergebe er diese dem Postdienstleister. Bis zum Eingang beim Energieversorger hätten lediglich Angestellte des Postdienstleisters die Möglichkeit, von den Kundendaten Kenntnis zu nehmen. Nach Eingang beim Energieversorger werde die Postkarte von einer Mitarbeiterin direkt in Empfang genommen, bearbeitet, sortiert und abgeheftet. Diese Mitarbeiterin sei auf die Vertraulichkeit verpflichtet und auch im Datenschutz sensibilisiert worden.

Es verbleibe nur ein Risiko im Bereich des Postdienstleisters, so die Ausführungen des Verantwortlichen. Allerdings unterliegen die Mitarbeiter von Postdienstleistern strengen rechtlichen Vorgaben bei der Ausübung ihrer Tätigkeit, insbesondere dem Postgeheimnis (Postgesetz und Postdienste-Datenschutzverordnung). Dementsprechend sei den Post-Mitarbeiter*innen untersagt, sich oder anderen über das für die Erbringung der Postdienste erforderliche Maß hinaus Kenntnis vom Inhalt von Postsendungen – unabhängig davon, ob es sich um offene oder verschlossene Sendungen handelt – zu verschaffen.

Selbst wenn nach dieser Auffassung keine Datenübermittlung an eine unbestimmte Anzahl Dritter vorliegt, gewährt Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO eine Verarbeitung nur, sofern die Einholung der Werbeeinwilligung mittels Postkarte zur Wahrung der berechtigten Interessen des Energieversorgers erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern.

Bereits bei der Prüfung der Erforderlichkeit des Rückversandes mittels Postkarte scheitert es an der Zulässigkeit. Es steht ein milderes Mittel, nämlich der Rückversand in einem verschlossenen Umschlag, zur Verfügung. Diese Methode greift weniger in die Grundrechte und Grundfreiheiten der Kunden des Energieversorgers ein. Die Anforderung, die Einwilligungserklärung in einem verschlossenen Umschlag zurückzusenden, ist auch für den Energieversorger geeignet. Mit der Rücksendung in einem verschlossenen Umschlag ergibt sich für den Verantwortlichen zum bisherigen Verfahren der Rücksendung mittels Postkarte eine überschaubare Erhöhung der finanziellen Mittel. Der Energieversorger führte selbst aus, dass die Versendung der Postkarte in einem Briefumschlag den Kunden selbst zuzumuten sei, da es sich für den Kunden um ein überschaubares Porto handelt.
Im Ergebnis hat der Datenschutzbeauftragte des Energieversorgers empfohlen, künftig auf die Einholung der datenschutzrechtlichen Einwilligungen per Postkarte zu verzichten und ist damit den Forderungen des TLfDI nachgekommen.
Auch die vom TLfDI kritisierte Einwilligungserklärung für Werbezwecke wurde überarbeitet. Darin hat der Verantwortliche alle vom TLfDI geforderten Überarbeitungen umgesetzt. Aus der Einwilligung geht nunmehr deutlich hervor, dass diese freiwillig erfolgt und jederzeit für die einzelnen Kontaktwege und -zwecke mit Wirkung für die Zukunft widerrufen werden kann. Auf die Folgen der Verweigerung der Einwilligung weist der Energieversorger ausdrücklich und in einfacher Sprache mit dem Passus hin: „Wenn ich keine Einwilligung gebe, erfolgt keine Werbung in den beschriebenen Umfang und der beschriebenen Form.“ Die Kunden können in Form des Ankreuzens zwischen der Werbung in den Produktbereichen

- ☐ Strom,
- ☐ Gas und
- ☐ Produkte im Bereich der Energieberatung und Energieeffizienz wählen. Weiterhin haben die Kunden nun die Möglichkeit zwischen den Kontaktmöglichkeiten
- ☐ E-Mail,
- ☐ Telefon und
- ☐ Fax,

ebenfalls durch Ankreuzen, auszuwählen. Für den Kunden ist nunmehr deutlich erkennbar, auch anhand der Textgestaltung, dass es sich um eine Einwilligungserklärung handelt. Die Überschrift „Bitte hier abtrennen und zurücksenden, das Porto zahlen wir für Sie“ wurde

durch „Einwilligungserklärung zur Verarbeitung personenbezogener Daten“ ersetzt. Da der Energieversorger allen Forderungen des TLfDI nachgekommen ist, war nichts weiter zu veranlassen.

4.8 Welche Daten seiner Arbeitnehmer darf ein Arbeitgeber ans Thüringer Landesamt für Statistik übermitteln?

Ist ein Unternehmen nach Art. 15 Bundesstatistikgesetz in Verbindung mit § 8 Abs. 1 des Gesetzes über die Statistik der Verdienste und der Arbeitskosten über Beschäftigtendaten gegenüber dem Thüringer Landesamt für Statistik auskunftspflichtig, dann ist die Übermittlung der Daten an das Landesamt für Statistik datenschutzrechtlich zulässig. Das Einverständnis der Beschäftigten für die Übermittlung der Daten an das Thüringer Landesamt für Statistik ist nicht erforderlich.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage eines Unternehmens, ob es verpflichtet sei, zu Statistikzwecken an das Thüringer Landesamt für Statistik Daten der Beschäftigten wie Geschlecht, Geburtsjahr, Arbeitszeiten, Verdienstregelungen sowie die Rentenversicherungsnummer zu übermitteln. Die Benennung der Rentenversicherungsnummer wurde besonders kritisch gesehen, weil diese den Rückschluss auf den einzelnen Arbeitnehmer zuließ. Insbesondere wollte das Unternehmen wissen, ob es verpflichtet sei, das Einverständnis des jeweiligen Arbeitnehmers einzuholen und ob die Beschäftigten entsprechend Art. 14 Datenschutz-Grundverordnung (DS-GVO) zu informieren seien.
Zweck des Gesetzes über die Statistik der Verdienste und der Arbeitskosten (VerdStatG) ist nach § 1 VerdStatG die Durchführung wirtschaftspolitischer Planungsentscheidungen zur Erfüllung von Berichtspflichten nach dem Recht der Europäischen Gemeinschaften zur Erstellung einer Bundesstatistik der Arbeitsverdienste und Arbeitskosten. Nach § 4 VerdStatG können durch das Landesamt für Statistik wahlweise folgende Beschäftigtendaten erhoben werden:

a) Geschlecht,
b) Geburtsjahr,
c) Monat des Eintritts in die Erhebungseinheit, bei Teileinheiten der Monat des Eintritts in die jeweilige Gesamteinheit,
d) ausgeübter Beruf,
e) höchster Bildungsabschluss,

f) Vergütungs- oder Leistungsgruppe,
g) Art des Beschäftigungsverhältnisses,
h) vertraglich vereinbarte wöchentliche Arbeitszeit,
i) Zahl der bezahlten Arbeitsstunden mit getrennt ausgewiesenen Überstunden,
j) Bruttomonatsverdienst, untergliedert nach Verdienstbestandteilen,
k) Bruttojahresverdienst, untergliedert nach Verdienstbestandteilen sowie die Zahl der Wochen, auf die sich der Bruttojahresverdienst bezieht,
l) Zahl der jährlich zu beanspruchenden bezahlten Urlaubstage,
m) angewandte Vergütungsvereinbarung.

Die Daten werden für Untersuchungen zu den Themen Niedriglohnsektor, unterschiedliche Bezahlung von Männern und Frauen sowie betriebliche Altersvorsorge durch Entgeltumwandlung erhoben.

Der TLfDI konnte nach Prüfung aller Unterlagen feststellen, dass die Verarbeitung der personenbezogenen Daten, insbesondere der Rentenversicherungsnummer, nicht zu beanstanden war. Dies begründete der TLfDI folgendermaßen:

Gemäß Art. 6 Abs. 3 DS-GVO kann der nationale Gesetzgeber Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten erlassen, soweit nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist und im öffentlichen Interesse liegt. Nach Art. 6 Abs. 3 Buchstabe b) DS-GVO muss der Zweck der Verarbeitung festgelegt und die Verarbeitung der personenbezogenen Daten erforderlich sein.

Zur Ermittlung einer statistischen Grundlage des Verdiensts sind neben der Erhebung der Daten zum Verdienst, Daten zu Wochenarbeitsstunden, Arbeitszeit, Urlaubstagen und Art des Beschäftigungsverhältnisses erforderlich. Zur Erstellung von Statistiken zur gleichen Bezahlung von Männern und Frauen ist neben dem Geschlecht auch die Frage des Bildungsabschlusses, des Alters und des Eintritts in die Erhebungseinheit (also Beginn des Arbeitsverhältnisses im jeweiligen Bereich) erforderlich, um eventuelle Ungleichheiten bewerten zu können.

Die statistisch ermittelten Daten dienen wiederum als Grundlage, um politische und gesetzgeberische Entscheidungen zu treffen und den Arbeitsmarkt im Sinne der Reduzierung von Ungerechtigkeiten zu beeinflussen. Dieses öffentliche Interesse kann mithilfe der Verarbeitung der oben genannten Daten erreicht werden.

Neben den in §§ 3 und 4 VerdStatG genannten Erhebungsmerkmalen sind auch die Hilfsmerkmale nach § 7 VerdStatG zu übermitteln. Nach dem ausdrücklichen Wortlaut des § 7 Nr. 3 VerdStatG gehören hierzu auch die Versicherungsnummer der gesetzlichen Rentenversicherung oder, wenn keine Versicherung in der gesetzlichen Rentenversicherung vorliegt, die Namen der Beschäftigten. Damit die erhobenen statistischen Zahlen verlässlich sind, werden die Angaben bei den Arbeitgebern unter gesetzlicher Auskunftspflicht gewonnen und gründlich überprüft. Die Rentenversicherungsnummern sollen eine Nachfrage des Thüringer Landesamtes für Statistik ermöglichen und Verwechslungen verhindern. Sie werden als Hilfsmerkmale nach § 10 Bundesstatistikgesetz (BstatG) in Verbindung mit § 7 VerdStatG erhoben. Diese Hilfsmerkmale sind Angaben, die lediglich der statistischen Durchführung dienen und nach Prüfung auf Schlüssigkeit von den Erhebungsmerkmalen zu trennen und frühestmöglich zu löschen sind. Auch dieses Vorgehen beanstandet der TLfDI nicht.
Zudem teilte der TLfDI dem Anfragenden mit, dass das Einverständnis des jeweiligen Beschäftigten zur Übermittlung der Daten an das Thüringer Landesamt für Statistik nicht erforderlich sei. Dabei hat der TLfDI zunächst festgestellt, dass das Unternehmen gemäß Art. 15 BStatG in Verbindung mit § 8 Abs. 1 VerdStatG gegenüber dem Landesamt für Statistik auskunftspflichtig war. Die durch das Unternehmen bereits erhobenen Daten konnten auf der Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Verbindung mit Art. 6 Abs. 3 Buchstabe b) DS-GVO, § 8 VerStatG, § 15 BstatG an das Thüringer Landesamt für Statistik weitergegeben werden.
Weiterhin wurde dem anfragenden Unternehmen mitgeteilt, dass es im Rahmen der Informationspflichten nach Art. 13 DS-GVO zum Zeitpunkt der Erhebung der Daten beim Betroffenen (Beginn des Datenverarbeitungsprozesses, also bei Anstellung des Beschäftigten) mitteilen muss, zu welchem Zweck die Daten erhoben und an welche Empfänger die Daten übermittelt werden. Danach ist das Unternehmen verpflichtet anzugeben, dass nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Verbindung mit Art. 6 Abs. 3 Buchstabe b) DS-GVO, § 8 VerdStatG, § 15 BStatG Daten an das Thüringer Landesamt für Statistik übermittelt werden. Des Weiteren muss das Unternehmen im Rahmen des Verarbeitungsverzeichnisses nach Art. 30 DS-GVO aufnehmen, dass Daten zum Zwecke statistischer Erhebungen an das Thüringer Landesamt für Statistik übermittelt werden.

Das Thüringer Landesamt für Statistik ist nach Art. 14 Abs. 5 Buchstabe c) DS-GVO jedoch nicht verpflichtet, den jeweiligen Bürger entsprechend Art. 14 DS-GVO, darüber zu informieren, dass es seine personenbezogenen Daten verarbeitet. Nach Art. 14 Abs. 5 Buchstabe c) DS-GVO entfallen die Informationspflichten des Art. 14 DS-GVO wenn und soweit eine Rechtsvorschrift die Erhebung bestimmter personenbezogener Daten ausdrücklich regelt. Dies ist hier der Fall.

4.9 GPS-Überwachung im Dienstfahrzeug

Die Ortung von Dienstfahrzeugen von Mitarbeitern eines Unternehmens ist nur zulässig, wenn der betroffene Mitarbeiter über die Maßnahme im Rahmen des Art. 13 Datenschutz-Grundverordnung informiert wird und aufgrund eines für den Mitarbeiter vorliegenden Vorteils von einer freiwillig erteilten Einwilligung ausgegangen werden kann.

Zuständigkeitshalber wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) durch die Polizei folgender Sachverhalt weitergeleitet: Der Geschäftsführer eines Thüringer Unternehmens überließ einem Mitarbeiter zur dienstlichen und privaten Nutzung einen Firmen-PKW. Ohne Kenntnis des Mitarbeiters ließ der Geschäftsführer an dem überlassenen Fahrzeug einen GPS-Sender verbauen. Dieser GPS-Sender übermittelte Daten zur Fahrstrecke, zu Haltepunkten sowie zu den jeweiligen Uhrzeiten an den Geschäftsführer des Unternehmens. Dieser überwachte damit den betroffenen Mitarbeiter dienstlich und privat und erstellte darüber hinaus ein Bewegungsprofil. Damit verarbeitete der Geschäftsführer des Unternehmens ohne Wissen des betreffenden Mitarbeiters personenbezogene Daten, so zum Beispiel Fahrzeit, Haltepunkte, Pausenzeiten sowie Arbeitszeiten. Gemäß Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) müssen personenbezogene Daten u. a. auf rechtmäßige Weise verarbeitet werden. Eine Rechtmäßigkeit liegt gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO vor, wenn die Einwilligung des Betroffenen vorliegt oder ein sonstiger Rechtsgrund nach Art. 6 Abs. 1 Satz 1 DS-GVO greift.
Durch die GPS-Überwachung wird in das Recht der informationellen Selbstbestimmung des betroffenen Mitarbeiters eingegriffen. Die

Fahrzeugdaten, welche der GPS-Sender übermittelt, sind dem konkreten Mitarbeiter zuzuordnen, da nur dieser das Fahrzeug dienstlich und privat benutzt.
Bei der GPS-Überwachung in Dienstfahrzeugen ist zudem den Aspekten des Beschäftigtendatenschutzes gemäß § 26 Bundesdatenschutzgesetz (BDSG) Rechnung zu tragen. Danach dürfen personenbezogene Daten nur zum Zweck des Beschäftigungsverhältnisses verarbeitet werden. Im vorliegenden Fall ist darauf zu achten, zu welchem Zweck die GPS-Überwachung angewendet wird. Die Beschäftigtenkontrolle durch Ortungssysteme ist datenschutzrechtlich nur in sehr engen Grenzen zulässig. Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten, welche durch einen GPS-Sender ermittelt worden sind, kann grundsätzlich nicht auf die Einwilligung des Beschäftigten gestützt werden. Eine Einwilligung im Sinne der Art. 6 Abs. 1 Satz 1 Buchstabe a) und 7 DS-GVO bedarf verschiedener Anforderungen. Diese muss durch den Verantwortlichen nachweisbar sein, sie muss von anderen Sachverhalten leicht zu trennen sein, es muss das Recht des Widerrufes eingeräumt werden und sie muss freiwillig erteilt werden.
Problematisch ist in dem Zusammenhang die Freiwilligkeit der Einwilligung. Aufgrund des Über- / Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer kann eine Abhängigkeit vorliegen, welche die Freiwilligkeit ausschließt. Nach der Ansicht des TLfDI liegt eine Freiwilligkeit vor, wenn sich gleichgelagerte Interessen gegenüberstehen oder der Beschäftigte darüber hinaus einen rechtlichen oder wirtschaftlichen Vorteil erlangt, § 26 Abs. 2 BDSG. Im vorliegenden Fall bestand zwischen dem Mitarbeiter und dem Arbeitgeber ein Dienstfahrzeugs-Nutzungsvertrag im Rahmen der 1-Prozent-Lösung. Das bedeutet, der Mitarbeiter durfte das Fahrzeug auch privat nutzen, musste dafür aber monatlich 1 Prozent des Listenpreises des überlassenen Fahrzeuges versteuern. Grundsätzlich wäre dies ein Vorteil, welcher zu einer Freiwilligkeit der Einwilligung führen würde. Allerdings wurde die Verarbeitung der personenbezogenen GPS-Daten ohne Wissen des Mitarbeiters durchgeführt, sodass weder eine Einholung der Einwilligung erfolgte, noch der Informationspflicht nach Art. 13 DS-GVO durch den Geschäftsführer des Unternehmens nachgekommen wurde.
Dieses Verhalten ist als unzulässig einzuordnen, was die Verhängung eines Bußgeldes zur Folge hatte.

4.10 Dürfen Recyclingunternehmen Personalausweiskopien anfertigen?

Voraussetzung für die zulässige Anfertigung von Personalausweiskopien ist grundsätzlich die Einwilligung des Ausweisinhabers zur Ablichtung sowie die Erkennbarkeit dieser als Kopie. Im zweiten Schritt muss eine Einwilligung zur Datenverarbeitung der gewonnenen Ausweisdaten entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe a) Datenschutz-Grundverordnung eingeholt werden. Zuletzt müssen zudem die technischen und organisatorischen Maßnahmen bei der Speicherung und Löschung der erhaltenen Daten beachtet werden.

Im Berichtszeitraum erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) einige Anfragen zur Zulässigkeit von Fotokopien von Personalausweisen. Unter anderem beschwerte sich ein Bürger beim TLfDI darüber, dass bei der Abgabe von Schrott eine Kopie seines Personalausweises gefertigt wurde. Der Betroffene hatte bei einem Recyclingunternehmen Schrott- und Buntmetalle gegen Vergütung abgeben. Die Vergütung hatte er jedoch erst ausbezahlt bekommen, als er sich mittels Personalausweis ausgewiesen und der Anfertigung eine Personalausweiskopie zugestimmt hatte.
Der Beschwerdeführer wollte vom TLfDI nun wissen, ob es zulässig sei, dass der Recyclinghof die Ausweiskopie gefertigt hat und ob dieser die Kopie aufbewahren dürfte. Da der Betroffene dem TLfDI die Kontaktdaten des Recyclingunternehmens nicht mitteilte, konnte sich der TLfDI nicht direkt an das Unternehmen wenden. Dem Beschwerdeführer wurde deshalb allgemein zur Frage „Anfertigung von Personalausweiskopien“ geantwortet.
Bereits im 1. Tätigkeitsbericht zum Datenschutz nach der Datenschutz-Grundverordnung (DS-GVO) aus dem Jahre 2018 (Seite 176) hat sich der TLfDI mit der Frage von Schwärzungen von Personalausweiskopien beschäftigt. Seit dem 14. Juli 2017 gilt eine neue Rechtslage zur Frage der Zulässigkeit von Personalausweiskopien. Demgemäß dürfen nach § 20 Abs. 2 Personalausweisgesetz (PAuswG) Kopien nur vom Ausweisinhaber oder von Dritten mit Zustimmung des Ausweisinhabers anfertigt werden. Dabei muss die Ablichtung eindeutig und dauerhaft als Kopie erkennbar sein. Voraussetzung ist also zunächst die Einwilligung nach § 20 Abs. 2 PAuwG des Ausweisinhabers zur Ablichtung, dies umfasst auch die Erstellung einer Fotoko-

pie sowie die Erkennbarkeit dieser als Kopie (zum Beispiel als Schwarz-Weiß-Druck).
Zudem muss der Ausweisinhaber die Erlaubnis zur Verarbeitung der der Ausweiskopie zu entnehmenden Daten entsprechend den Vorgaben der DS-GVO erteilen oder die Datenverarbeitung durch den Verantwortlichen muss zur Erfüllung einer rechtlichen Pflicht erforderlich sein (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO). Die Erstellung einer Fotokopie eines Personalausweises stellt eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DS-GVO dar. Als Rechtsgrundlage für die Verarbeitung der Ausweisdaten kommt entweder eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO oder die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Betracht.
Eine Einwilligung lag mangels Freiwilligkeit hier nicht vor. Eine Einwilligung nach Art. 7 DS-GVO muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden. Freiwillig ist eine Einwilligung dann, wenn der Betroffene eine echte Wahl hat, ob er eine Leistung vom Unternehmen erhält, auch wenn er seine personenbezogenen Daten nicht zur Verfügung stellt. Wird der Vertragsabschluss jedoch von der Einwilligung zur Verarbeitung weiterer personenbezogener Daten abhängig gemacht, geht der Betroffene folglich das Risiko ein, dass ihm Leistungen verwehrt werden. Entsprechend dem sogenannten Kopplungsverbot, ist eine solche Einwilligung weder freiwillig noch wirksam. Zudem muss im Vorfeld zur Einwilligungserklärung festgestellt werden, welchen Umfang der Vertrag hat und welche Daten für die Erfüllung des Vertrages erforderlich sind. Hierüber muss der Betroffene informiert werden. Im vorliegenden Fall wurde die Zahlung der Vergütung von der Anfertigung der Personalausweiskopie abhängig gemacht. Dem Betroffenen wurde nicht erläutert, warum alle Daten, die sich aus dem Personalausweis ergeben, für die Abwicklung des Vertrages – Abgabe von Schrott und Buntmetallen – zwingend erforderlich seien.
Auch eine zulässige Datenverarbeitung auf der Grundlage des Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit § 143 Abs. 3 Abgabenordnung (AO) zur Erfüllung einer rechtlichen Verpflichtung des Recyclingunternehmens kam nicht in Betracht. Zwar sind grundsätzlich nach § 143 Abs. 3 AO gewerbliche Unternehmer, auch Recyclingunternehmen/Schrotthändler, verpflichtet, Aufzeichnungen über ihre Warengänge zu machen. Unter anderem sind Name und An-

schrift des Lieferanten sowie der Tag der Abgabe zu notieren. Die Aufzeichnung weiterer personenbezogener Daten wird nach § 143 AO nicht gefordert. Da der Personalausweis eine Vielzahl weiterer Daten enthält, schied ein Verarbeitungsrecht nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit § 143 Abs. 3 AO folglich aus.
Auch auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Verbindung mit § 160 AO konnte die Anfertigung einer Ausweiskopie nicht gestützt werden. Gemäß § 160 AO können die Finanzbehörden einen Steuerpflichtigen auffordern, den Empfänger von Betriebsausgaben zu benennen. Um dieser Aufforderung im Zweifel nachkommen zu können, musste das Recyclingunternehmen personenbezogene Daten des Beschwerdeführers erheben. Zweck des § 160 AO ist, die damit korrespondierenden Einnahmen beim Geschäftspartner zu erfassen, um Steuerausfälle zu verhindern. Hierfür ist es ausreichend, dass eine Person ohne Schwierigkeiten bestimmt und ermittelt werden kann (BFH Urt. V. 20. April 2005 X R 40/04). Dies ist mittels Namens- und Adressaufzeichnung hinreichend möglich. Zur Kontrolle der Angaben des Beschwerdeführers war es mithin für das Recyclingunternehmen zulässig, sich den Personalausweis vorlegen zu lassen, die Anfertigung einer Ausweiskopie war jedoch nicht notwendig.
Die Anfertigung einer Personalausweiskopie konnte weiterhin nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 DS-GVO in Verbindung mit § 8 Abs. 2 Geldwäschegesetz (GwG) gestützt werden. Sofern „zur Überprüfung der Identität einer natürlichen Person Dokumente nach § 12 Abs. 1 Satz 1 Nummer 1 [Personalausweis] vorgelegt oder herangezogen werden, haben die Verpflichteten das Recht und die Pflicht, vollständige Kopien dieser Dokumente oder Unterlagen anzufertigen oder sie vollständig optisch digitalisiert zu erfassen.“ Zur Anfertigung einer Personalausweiskopie verpflichtet sind nach § 2 Abs. 1 GwG unter anderem Kreditinstitute, Finanzdienstleister, Versicherungsvermittler und Immobilienmakler. Das Recyclingunternehmen/Schrotthändler war kein Verpflichteter nach § 2 Abs. 1 GwG und konnte sich bei der Anfertigung der Personalausweiskopie nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Verbindung mit § 8 Abs. 2 GwG berufen.
Dem Betroffenen wurde daher mitgeteilt, dass nach Ansicht des TLfDI nach dem vorgetragenen Sachverhalt keine Rechtsgrundlage für die Anfertigung einer Ausweiskopie gegeben war. Er wurde im Weiteren darauf hingewiesen, dass ihm ein Auskunftsrecht nach Art. 15 DS-GVO gegenüber dem Recyclingunternehmen zusteht. Mit

der Auskunftserteilung ist erkennbar, welche personenbezogenen Daten durch das Recyclingunternehmen gespeichert und an wen gegebenenfalls Daten übermittelt wurden. Des Weiteren wurde er darüber informiert, dass ihm nach Art. 17 DS-GVO ein Anspruch auf Löschung der Daten zusteht, die zur Zweckerreichung nicht notwendig sind. Entsprechend der zuvor gemachten Ausführungen wurde der Beschwerdeführer darauf hingewiesen, dass er zudem die Vernichtung der Personalausweiskopie verlangen könnte.
Weitere problematische Fragen, wie die Speicherung der Personalausweiskopien, die Umsetzung der technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten oder die Frage nach Löschkonzepten konnten mangels weiterführender Angaben zum Recyclingunternehmen nicht geklärt werden.

4.11 Gefahr erkannt beim Faxversand

Die Offenlegung einer Faxnummer im Rahmen einer Einladung zu einer politischen Veranstaltung ist eine Verarbeitung eines personenbezogenen Datums besonderer Kategorie gemäß Art. 9 Datenschutz-Grundverordnung. Es reicht aus, dass dieses Datum die Annahme stützt, dass der Inhaber der Faxnummer eine bestimmte politische Zugehörigkeit aufweist.

Im Rahmen der behördlichen Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte dieser Kenntnis über eine fehlerbehaftete Einladung einer Partei zu einer alljährlichen politischen Veranstaltung.
Im Dezember 2018 lud diese Partei ca. 300 Unternehmer, Bürger und politisch aktive Personen zu einer gemeinsamen Veranstaltung ein. Auf der als Anlage zur Einladung angefügten Rückantwort wurde allerdings nicht die Faxnummer der Geschäftsstelle dieser Partei angegeben, sondern die private Faxnummer eines seit Jahren aus der Partei ausgetretenen ehemaligen Mitgliedes.
Die Offenlegung dieser privaten Faxnummer auf dem Rückantwortschreiben zu der traditionellen Veranstaltung stellt einen Verstoß gegen Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) dar, nach dem personenbezogene Daten über politische Meinungen nur in wenigen Ausnahmefällen verarbeitet werden dürfen. Die Faxnummer ist ein personenbezogenes Datum gemäß Art. 4 Nummer 1 DS-GVO, weil sie sich auf eine identifizierbare natürliche Person bezieht.

Gleichzeitig wird mit der Offenlegung auch die politische Zugehörigkeit zu der Partei verknüpft, die die Veranstaltung durchführt. Die politische Meinung gehört zu den personenbezogenen Daten besonderer Kategorie gemäß Art. 9 Abs. 1 DS-GVO, deren Verarbeitung grundsätzlich untersagt ist. Das Verarbeitungsverbot gilt für alle Daten, aus denen sensible Aspekte hervorgehen. Dabei genügt es, wenn sich die politische Verknüpfung mittelbar aus dem Gesamtzusammenhang ergibt. Das Einladungsschreiben wurde von der Geschäftsstelle der Partei organisiert. Das Rückanwortschreiben zur Teilnahme ist ebenfalls an diese zu richten gewesen. Dabei kann davon ausgegangen werden, dass der Anschlussinhaber der Faxnummer der einladenden Partei zuzuordnen ist.
Vollkommen irrelevant ist es, ob die Information wahrheitsgemäß ist oder nicht. Es ist ausreichend, dass eine vermeintliche politische Zugehörigkeit offengelegt oder suggeriert wird.
Aufgrund der rechtswidrigen Verarbeitung der Faxnummer und der Tatsache, dass die Partei nach Bekanntwerden dieser Datenpanne keine Meldung nach Art. 33 Abs. 1 DS-GVO vorgenommen hat, wurde durch den TLfDI im Rahmen des Verwaltungsverfahrens gegen den Kreisverband der Partei eine kostenpflichtige Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO erlassen.

4.12 Veröffentlichung von Vereinsprotokollen in Schaukästen

Bei der Beurteilung der Zulässigkeit von Aushängen in Schaukästen spielt es keine Rolle, ob es sich dabei um Vereinsschaukästen handelt oder nicht. Vielmehr kommt es auf den Inhalt der Informationen an. Personenbezogene Daten dürfen mit einem Aushang nur übermittelt werden, wenn es zur Erfüllung der Vereinsmitgliedschaft erforderlich ist, Art. 6 Abs. 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung. Beim Aushängen in Schaukästen handelt es sich nämlich um eine Übermittlung an einen unbestimmten Personenkreis.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde darüber, dass der Vorstand eines Kleingartenvereins als Verantwortlicher das Protokoll einer Vorstandssitzung öffentlich bekanntgemacht hat. Dafür wurde das Protokoll in insgesamt drei Schaukästen ausgehangen. Darin wurden die Teilnehmer abgekürzt mit dem ersten Buchstaben des Vornamens und mit dem Nachnamen aufgeführt. Die Teilnehmer hatten in

die Veröffentlichung ihrer personenbezogenen Daten nicht eingewilligt.
Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Dazu gehören ebenfalls Angaben zur sozialen Identität einer betroffenen Person. Dem Protokoll waren zweifelsfrei die Teilnehmer zu entnehmen. Diese waren im Protokoll mit Namensangabe und dem abgekürzten Vornamen niedergeschrieben. Weiterhin erfolgte zum Namen eine Zuordnung, für welchen Verein oder welche Institution der Teilnehmer anwesend war. Weiterhin ließ es darauf schließen, welche Teilnehmer Mitglied des Kleingartenvereins sind und es waren aufgrund der Äußerungen in der Sitzung Rückschlüsse auf Lebenssachverhalte möglich.
Der Aushang in den Vereinsschaukästen stellt eine Verarbeitung personenbezogener Daten, in Form einer Verbreitung, dar (Art. 4 Nr. 2 DS-GVO). Bei dieser Beurteilung spielt es keine Rolle, dass es sich um Schaukästen des Kleingartenvereins handelte. Vielmehr liegt eine Verbreitung personenbezogener Daten vor, wenn diese an eine unbestimmte Vielzahl von Empfängern weitergeben werden. Dies ist hier geschehen, da die Schaukästen der Ortslage für jedermann öffentlich zugänglich sind.
Die Übermittlung der oben genannten personenbezogenen Daten ist nur erlaubt, soweit sie zur Vertragserfüllung (Pachtvertrag im Kleingartenverein) erforderlich ist oder eine Rechtsvorschrift sie vorsieht, Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO. Zur Erfüllung des Pachtvertrages ist die Verbreitung des oben genannten Protokolls ebenfalls nicht erforderlich, auch wenn für die Pächter wichtige Informationen darin enthalten waren. Diese Informationen hätten auch auf eine weniger in die Rechte und Freiheiten der betroffenen Personen einschneidende Art und Weise an die Pächter weitergegeben werden können. Zum Beispiel durch den Aushang in den Schaukästen mit dem Ergebnis der Vorstandssitzung ohne Personenbezug.
Letztlich wurden die Protokolle nach Aufforderung des TLfDI aus den Schaukästen der Ortslage entfernt und es konnte ein datenschutzgerechter Zustand wiederhergestellt werden. Der Verein sagte zu, künftig die Protokolle ohne Personenbezug in den Schaukästen auszuhängen.

4.13 Antrag auf Auskunftserteilung nur gegen Kostenübernahme?

Die erstmalige Auskunft nach Art. 15 Abs. 1 Datenschutz-Grundverordnung der beantragenden betroffenen Person ist grundsätzlich unentgeltlich durch den Verantwortlichen zu erteilen. Kosten können seitens des Verantwortlichen nur bei unbegründeten oder exzessiven Anträgen verlangt werden. Hierfür trägt der Verantwortliche die Beweislast. Eine Kostentragung der betroffenen Personen ergibt sich auch aus der Beantragung von weiteren Datenkopien, welche jedoch nicht die erste Datenkopie beinhaltet.

Im Juni 2019 erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über hundert Beschwerden zu einer Rechtsanwaltskanzlei. Gläubiger aus einem Insolvenzverfahren hatten gegenüber dieser Rechtsanwaltskanzlei einen Formularantrag zur Auskunftserteilung nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) gestellt. Die Anwaltskanzlei hatte diese Antragsteller angeschrieben und den Eindruck vermittelt, dass die Auskunft nach Art. 15 DS-GVO Kosten verursachen könnte. Dem Schreiben war ein entsprechender Antwortbogen beigefügt. Darin wurde die geforderte Auskunft für gegenstandslos erklärt. Weiterhin wurde eine Kostentragungspflicht durch den Antragsteller abgelehnt und gleichzeitig wurde mit der Rücksendung des Antwortbogens die Kanzlei stattdessen beauftragt eine Auskunft nach Art. 15 DS-GVO bei dem insolventen Unternehmen zu beantragen. Sofern der Antwortbogen nicht zurückgesendet werden würde, erfolge eine Prüfung und Bearbeitung, auch wenn hierdurch nicht unerhebliche Kosten nach Art. 15 Abs. 3 DS-GVO entstehen könnten. Die Betroffenen wandten sich deswegen an den TLfDI und fragten an, ob hier tatsächlich Kosten für die beantragte Auskunft verlangt werden könnten. Die Verunsicherung war sehr groß.

Der TLfDI musste in diesem Fall unverzüglich tätig werden, da die Rechtsanwaltskanzlei die Rücksendung des Antwortbogens innerhalb einer kurzen Frist vorsah. Mit der Vorgehensweise der Rechtsanwaltskanzlei sollten die Betroffenenrechte nach der DS-GVO umgangen werden. Dem nicht unerheblichen Arbeitsaufwand hinsichtlich einer zu erteilenden Auskunft in einem Verfahren mit tausenden von Gläubigern sollte daneben ebenfalls entgangen werden. Auch wenn die Formulierung im Schreiben der Rechtsanwaltskanzlei im Konjunktiv

erfolgte, wurde hier den betroffenen Personen eine Kostentragungspflicht für die zu erteilende Auskunft suggeriert. Dabei wurden diese bewusst irregeführt und durch die Notwendigkeit der Rücksendung des Antwortbogens zur Aufgabe ihrer Rechte gebracht. Darin ist ein gravierender Verstoß gegen die DS-GVO zu sehen. Mittels kostenpflichtiger Anordnung wurden die Rechtsanwälte dazu verpflichtet, die erstmalige Auskunft nach Art. 15 DS-GVO unentgeltlich gegenüber den Betroffenen zu erteilen.

Nach Art. 12 Abs. 5 Satz 1 DS-GVO hat die Auskunft nach Art. 15 Abs. 1 DS-GVO grundsätzlich unentgeltlich zu erfolgen. Nur bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen kann der Verantwortliche für die Auskunft ein angemessenes Entgelt verlangen. Bei einer erstmaligen Auskunftserteilung nach Art. 15 Abs. 1 DS-GVO liegen diese Voraussetzungen nicht vor. Ein hoher Bearbeitungsaufwand aufgrund der Anzahl der eingehenden Anträge führt nicht dazu, dass es sich um einen exzessiven Antrag jeder einzelnen Person handelt. Da die Rechtsanwälte zum Teil Gläubiger in dem Insolvenzverfahren bereits mit einem Informationsschreiben angeschrieben hatten, war auch nicht von vornherein auszuschließen, dass diese die Daten der betroffenen Gläubiger verarbeiten würden. Ein unbegründeter Antrag war danach auch nicht gegeben. Die Kostenfolge konnte auch nicht mit Art. 15 Abs. 3 Satz 2 DS-GVO begründet werden. Dieser sieht vor, dass der Verantwortliche für jede weitere Datenkopie ein angemessenes Entgelt verlangen darf. Eine Datenkopie nach Art. 15 Abs. 3 DS-GVO wurde seitens der betroffenen Personen nicht beantragt und gefordert, sodass diese Kostenfolge auch ausgeschlossen war.

Aufgrund der sofortigen Vollziehbarkeit der Anordnung wurden in der Folge seitens der Rechtsanwaltskanzlei die geforderten Auskünfte kostenfrei an die betroffenen Personen erteilt. Die sofortige Vollziehung wurde hier angeordnet, da es sich um einen sehr gravierenden Verstoß gegen die DS-GVO handelte. Hier sollten durch die gewählte Formulierung der Rechtsanwälte die gesetzlich bestehenden Verpflichtungen umgangen werden. Ziel des Schreibens war offensichtlich, die betroffenen Personen dazu zu bringen, auf ihre Rechte zu verzichten. Dies bedeutet eine Vereitelung der gesetzlich vorgeschriebenen Pflichten des Verantwortlichen und somit einen intensiven Eingriff in die Grundrechte der betroffenen Personen. Allein aus diesem Umstand sollte der Verantwortliche nicht durch Einlegung eines Rechtsbehelfs erreichen, dass er bis zur Rechtskraft der gerichtlichen

Entscheidung diese Verpflichtung nicht erfüllen muss. Die Auskunftserteilung wäre damit auf Eis gelegt – das wurde durch die Anordnung der sofortigen Vollziehung vermieden. Hierdurch wurde den Betroffenen effizient zu ihrem Recht auf Auskunft verholfen. Der Bescheid des TLfDI ist noch nicht rechtskräftig, da hiergegen Klage eingereicht wurde.

4.14 Dürfen Berufsgeheimnisträger Daten per E-Mail senden?

Bei der Versendung von E-Mails müssen die in der Datenschutz-Grundverordnung (DS-GVO) enthaltenen Pflichten zur Datensicherheit gemäß Art. 5 Abs. 1 Buchstabe f) in Verbindung mit Art. 32 Abs. 1 DS-GVO eingehalten werden. Hierfür ist die verschlüsselte Versendung von E-Mails dringend geboten. Dies gilt für Rechtsanwälte, die das Berufsgeheimnis nach § 203 Abs. 1 Nr. 3 Strafgesetzbuch (StGB) zu wahren haben, in besonderer Weise.

Rechnungen, Bilder und andere vertrauliche Dokumente sind schnell per E-Mail an den weit entfernten Empfänger gesendet. Natürlich vereinfacht die Übersendung von Dokumenten per E-Mail die Geschäftsabwicklungen und die Kommunikation. Wie steht es dabei aber um die Sicherheit der übermittelten Daten? Eine Frage, die sich viele vor der Versendung von personenbezogenen Daten per E-Mail nicht stellen.
So auch in einem dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt gewordenen Fall einer Wirtschafts- und Unternehmensberatungskanzlei, welche als Rechtsvertreter tätig wird. Diese wurde von ihrer Mandantin beauftragt, ein Schulungszertifikat anzufordern. Die Mandantin hatte bei einem Nagelstudio eine Schulung absolviert. Nach Zahlung der Rechnung wurde das Zertifikat hierfür jedoch nicht ausgestellt. Nunmehr wandte sich die Kanzlei an das Nagelstudio und übermittelte die Rechnung zu der Schulung in einer unverschlüsselten E-Mail mit Benennung der Schulungsleiterin (vorname.nachname@nagelstudio.de). Problematisch war bei diesem Fall weiterhin, dass die Schulungsleiterin zwischenzeitlich nicht mehr für das Nagelstudio tätig war. Vielmehr eröffnete sie ihren eigenen Nagelsalon. Die Schulungsleiterin beschwerte sich beim TLfDI vorwiegend darüber, dass ihre personenbezogenen Daten an das Nagelstudio übermittelt worden sind, obwohl

sie zum Zeitpunkt der Übermittlung per E-Mail nicht bei diesem tätig war.
Der TLfDI stellte grundsätzlich klar, dass das Schulungszertifikat bei dem Nagelstudio anzufordern war, weil dort die Schulung stattgefunden hatte. Die Anforderung war auch erforderlich, weil die Mandantin ebenfalls ein eigenes Unternehmen gründen wollte. Das Schulungszertifikat war eine Voraussetzung für die beabsichtigte Unternehmensgründung. Die Wirtschafts- und Unternehmensberatungskanzlei wurde von ihrer Mandantin beauftragt, sie bei der Unternehmensgründung zu unterstützen.
Die Übermittlung der besagten Rechnung an das Nagelstudio durch die Kanzlei kann rechtmäßig sein, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Mandantin der Kanzlei) erforderlich ist, sofern nicht die Grundrechte und Grundfreiheiten der Schulungsleiterin überwiegen, die den Schutz personenbezogener Daten erfordern, Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Eine vertragliche Rechtsgrundlage kommt nicht in Betracht, weil die Kanzlei mit der Schulungsleiterin keinen Vertrag geschlossen hatte. Die Datenübermittlung ist nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen erforderlich ist. Die Mandantin erhielt – trotz mehrfacher Aufforderung – im Anschluss an die Zahlung der Schulung kein Zertifikat. Da dieses Zertifikat aber für die Gründung eines Unternehmens zwingend erforderlich war, beauftragte die Mandantin die Wirtschafts- und Unternehmensberatungskanzlei mit der Durchsetzung ihrer Rechte. Hierfür legte die Mandantin ihre Rechnung zur Schulung vor. Die Kontaktaufnahme der Kanzlei über die E-Mail-Adresse der Schulungsleiterin war erforderlich, da die mildere Alternative – die persönliche Kontaktaufnahme – den gewünschten Zweck nicht erreicht hatte. Ihre Grundrechte am Schutz ihrer personenbezogenen Daten treten zu den Interessen der Kanzlei und der Mandantin zurück. Zumal in der von der Schulungsleiterin ausgestellten Rechnung die E-Mail-Adresse mit Zuordnung zum Nagelstudio als Kontaktmail angegeben wurde. Des Weiteren war die Schulungsleiterin als Inhaberin des Nagelstudios im Rechnungsformular aufgeführt. Nach dem Kenntnisstand des TLfDI hatte sie die auf ihr Zertifikat wartende Mandantin nicht darüber informiert, dass sie zwischenzeitlich nicht mehr mit dem Nagelstudio zusammenarbeitete und einen eigenen Nagelsalon eröffnet hatte.
Die Übermittlung der Rechnung an die E-Mail-Adresse mit Zuordnung zum Nagelstudio war im Ergebnis zulässig.

Dennoch müssen die in der Datenschutz-Grundverordnung enthaltenen Pflichten zur Datensicherheit gemäß Art. 5 Abs. 1 Buchstabe f) in Verbindung mit Art. 32 Abs. 1 DS-GVO eingehalten werden. Personenbezogene Daten, welche die Kanzlei im Rahmen ihrer Tätigkeit als Rechtsvertreter verarbeitet und die somit unter das Berufsgeheimnis fallen nach § 203 Strafgesetzbuch (StGB), müssen verschlüsselt per E-Mail versandt werden. Dies ergibt sich aus den Prinzipien der Vertraulichkeit und des Integritätsschutzes der Daten – verankert in Art. 5 Abs. 1 Buchstabe f) DS-GV – und den Regelungen zur Datensicherheit aus Art. 32 Abs. 1 DS-GVO. Unter Berücksichtigung des Standes der Technik, der Implementierungskosten sowie der Art, der Umstände und des Zweckes der Datenverarbeitung, aber auch der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten hat die Kanzlei als Verantwortliche für die Datenverarbeitung geeignete technische und organisatorische Maßnahmen umzusetzen. Dabei muss das Sicherheitsniveau im Verhältnis zum Risiko angemessen sein. Die Kanzlei hat die von ihrer Mandantin zur Verfügung gestellte Rechnung jedoch mit einer unverschlüsselten E-Mail an die E-Mail-Adresse mit Zuordnung zum Nagelstudio übermittelt.

Werden E-Mails weder während des Transports, Ende-zu-Ende verschlüsselt, noch signiert übermittelt, so können Schadensereignisse durch Angreifer bewirkt werden, die Zugriff auf mindestens ein System oder Netz besitzen oder unbefugt erlangt haben, das für die E-Mail-Übermittlung genutzt wird. Durch die Verschlüsselung kann die Vertraulichkeit der Daten im Sinne der Verhinderung der Kenntnisnahme durch einen unberechtigten Dritten erreicht werden. Die im Rahmen der Mandatsausübung zu verarbeitenden personenbezogenen Daten unterliegen dem Berufsgeheimnis nach § 203 StGB. Nur im Rahmen einer verschlüsselten elektronischen Versendung von Unterlagen im Rahmen eines Mandantenverhältnisses kann gewährleistet werden, dass das Berufsgeheimnis, dem die Wirtschafts- und Unternehmensberatungskanzlei gemäß § 203 Abs. 1 Nr. 3 StGB unterliegt, gewahrt wird. Alternativ dazu müssen andere als elektronische Kommunikationswege – beispielsweise die postalische Versendung – bevorzugt werden.

Daher hat der TLfDI aufgrund eines Verstoßes gegen Art. 32 Abs. 1 Buchstabe a) DS-GVO gegen die Wirtschafts- und Unternehmensberatungskanzlei gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO eine Verwarnung ausgesprochen.

4.15 Müssen nach einer Kündigung die Gemeinschaftsbilder entfernt werden?

Wird ein Gemeinschaftsbild für die Arbeitsräumlichkeiten angefertigt, muss die Verarbeitung nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) rechtmäßig und eine der Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO gegeben sein. Wenn die Rechtsgrundlage für die Fotoaufnahme eine Einwilligung der betroffenen Person ist, kann sie ihre Einwilligung nach Art. 7 Abs. 3 DS-GVO jederzeit widerrufen.

Im Januar 2019 wandte sich eine Arztpraxis an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um eine datenschutzrechtliche Einschätzung des folgenden Sachverhalts: Der Anfragende legte dar, dass eine Angestellte seiner Praxis gekündigt und daraufhin verlangt hatte, das Gemeinschaftsbild / Wandbild des Praxisteams, auf dem sie ebenfalls abgebildet war, aus datenschutzrechtlichen Gründen aus dem Sichtfeld der Patienten und aus der Praxis zu entfernen. Der Anfragende wollte wissen, ob die ehemalige Mitarbeiterin ein Anrecht darauf habe.
Da Fotoaufnahmen gemäß Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten darstellen, muss die Verarbeitung nach Art. 5 Abs. 1 Buchstabe a) DS-GVO rechtmäßig sein und es muss eine der Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO vorliegen. Da Angestellte einer Praxis nicht vertraglich verpflichtet sind, sich auf Fotos abbilden zu lassen, diente die Einwilligung der Mitarbeiterin als Rechtsgrundlage für die Fotoaufnahmen. Eine Einwilligung ist nur wirksam, wenn sie freiwillig, bezogen auf bestimmte Verarbeitungsvorgänge informiert abgegeben wird. Die Anforderungen einer Einwilligung sind in Art. 4 Nr. 11 und Art. 7 DS-GVO enthalten.
Nach Art. 7 Abs. 3 DS-GVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Allerdings ist jede weitere Datenverarbeitung nach Erklärung des Widerrufs unrechtmäßig.
Somit ist das Verlangen der ehemaligen Mitarbeiterin nach dem Entfernen des Teambildes als ein Widerruf zu interpretieren. Aus datenschutzrechtlicher Sicht ist daher der Wunsch gerechtfertigt und die

Praxis hat das Bild zu entfernen oder die abgebildete Person unkenntlich zu machen.

4.16 Datenschutz am Tresenbereich einer Arztpraxis

Wird am Empfang einer Arztpraxis mit dem Patienten über die Erkrankungen gesprochen, achten leider nicht alle darauf, ob es ein Dritter mithören könnte. Gemäß Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung müssen aber personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung. Um den Schutz der personenbezogenen Daten sicherzustellen, sollten sowohl die dazu erforderlichen technischen als auch organisatorischen Maßnahmen getroffen werden.

Im Juni 2019 wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und legte dar, dass er ein Patient in einer Praxis sei, welche zu einem medizinischen Versorgungszentrum (MVZ) gehöre. Der Beschwerdeführer berichtete, dass der Tresenbereich für die Anmeldung direkt neben einem weiteren Empfang einer anderen Praxis liege. So könne beim Anmelden an dem Empfangstresen jeder von den Anliegen des Patienten oder der anderen Personen Kenntnis erlangen.
Aufgrund des geschilderten Sachverhaltes könnte eine Verletzung des Schutzes der personenbezogenen Daten gemäß Art. 4 Nr. 12 Datenschutz-Grundverordnung (DS-GVO) vorliegen. Die Sicherheit der personenbezogenen Daten wird bei der Verarbeitung verletzt, wenn eine unbefugte Offenlegung beziehungsweise ein unbefugter Zugang zu den personenbezogenen Daten erfolgt. Dies ist der Fall, wenn andere Patienten Gespräche am Tresen mithören können.
Gemäß den Anforderungen des Art. 5 Abs. 1 Buchstabe f) DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. So müssen nach Art. 32 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen bestimmt und umgesetzt werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und somit auch die Vertraulichkeit und Integrität nach Art. 32 Abs. 1 Buchstabe b) DS-GVO sicherzustellen. Bei der Beurteilung des angemessenen Schutzniveaus nach Art 32 Abs. 2 DS-GVO sind insbesondere Risiken zu berück-

sichtigen, wie beispielsweise das mögliche Wahrnehmen der personenbezogenen Daten durch Dritte.
Aufgrund des Beschwerdevortrags bat der TLfDI das MVZ um eine Stellungnahme zu der möglichen Verletzung des Schutzes der personenbezogenen Daten und um eine konkrete Darlegung der räumlichen Gegebenheiten.
Daraufhin teilte das MVZ dem TLfDI mit, dass der vorliegende Sachverhalt sorgfältig geprüft wurde und diesbezüglich bauliche und organisatorische Umstrukturierungsmaßnahmen vorgenommen werden. Nach einer erneuten Nachfrage, wurde dem TLfDI mitgeteilt, dass die Anmeldungen der jeweiligen Praxen in separate Räume verlegt werden.

4.17 Das Haushaltsprivileg – keine Anwendung der DS-GVO im ausschließlich persönlichen und familiären Bereich

Finden Datenverarbeitungsvorgänge ausschließlich im persönlichen und familiären Bereich statt, so findet die DS-GVO keine Anwendung.

I. Allgemeines
Der auch als „Haushaltsprivileg“ bekannte Ausnahmetatbestand Art. 2 Abs. 2 Buchstabe c) Datenschutz-Grundverordnung (DS-GVO) schließt die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher und familiärer Tätigkeiten aus dem Anwendungsbereich der DS-GVO aus. Mit dieser Vorschrift bezweckt die DS-GVO einen Ausgleich zwischen den Grundrechten des Verarbeiters und der betroffenen Person. Dies gilt selbst dann, wenn besondere Kategorien personenbezogener Daten verarbeitet werden. Persönliche Tätigkeiten sind Tätigkeiten, die der eigenen Selbstentfaltung und Freiheitsausübung in der Freizeit oder im privaten Raum dienen. Familiäre Tätigkeiten sind alle Tätigkeiten, die der Pflege familiärer Beziehungen und des familiären Zusammenhalts dienen. Der Begriff familiär ist dabei nicht familienrechtlich auszulegen. Er umfasst unabhängig von Ehe, Kindschaft und Verwandtschaft jede Beziehung, die eine vergleichbare persönliche Nähe aufweist und von der Verkehrsanschauung als familiär angesehen wird.
Art. 2 Abs. 2 Buchstabe c) DS-GVO ermöglicht somit die Datenverarbeitung für den privaten und familiären Gebrauch. Insbesondere Urlaubsfotos, Fotoalben, Erinnerungsfotos, Stammbücher und Tagebü-

cher sind daher möglich, ohne die Voraussetzungen, die die DS-GVO für die Datenverarbeitung aufstellt, erfüllen zu müssen. Namen-, Adress- oder Geburtsdatensammlungen im Zusammenhang mit Freizeitaktivitäten, Hobbies, oder Urlaub fallen unter das Haushaltsprivileg. Diese Privilegierung fällt allerdings dann weg, wenn diese Informationen zu nicht mehr rein persönlichen oder haushaltsbezogenen Tätigkeiten verwendet werden, wie beispielsweise die Veröffentlichung im Internet.

II. Videoaufnahmen

Die Videoüberwachung privater und familiärer Lebensbereiche kann von der Ausnahme erfasst werden. So sind Aufnahmen, die lediglich im privaten Bereich verbleiben, also zum Beispiel als Erinnerung an bestimmte private Erlebnisse oder wenn die Videoüberwachung innerhalb der eigenen vier Wände stattfindet, grundsätzlich vom Haushaltsprivileg erfasst.

Jedoch ist der Wortlaut der Vorschrift des Art. 2 Abs. 2 Buchstabe c) DS-GVO sehr eng und hat lediglich einen sehr beschränkten Anwendungsbereich. Wird bei der Erstellung der Videoaufnahmen oder bei der Veröffentlichung der Aufnahmen in sozialen Netzwerken oder anderweitig der private und familiäre Kontext überschritten, greift das Haushaltsprivileg nicht und die DS-GVO findet Anwendung. Zwecke der Datenverarbeitung sind vorab festzulegen (Roßnagel in Simitis, Kommentar zum Datenschutzrecht, 1. Auflage, Art. 5, Rn. 72). Sobald im privaten Bereich eine Videoüberwachung Beweiszwecken dienen soll, wie beispielsweise bei einer Kameraüberwachung des eigenen Grundstücks, ist dies nicht mehr der reinen persönlichen oder familiären Tätigkeit zuzuordnen, da die persönliche und familiäre Sphäre aufgrund einer möglichen Übermittlung an die Strafverfolgungsbehörden verlassen wird (so auch Scholz in Simitis, Kommentar zum Datenschutzrecht, 1. Auflage, Anhang zu Art 6, Rn. 51). Anders ist die Zulässigkeit der Videoüberwachung zu beurteilen. Ist der Zweck der Videoüberwachung zunächst auf etwas anderes gerichtet, beispielsweise Beobachtung des eigenen Gartens, und wird sodann etwas Polizeirelevantes festgestellt und die Videodaten werden an die Polizei übermittelt, ist diese erneute Datenverarbeitung unter einer neuen Rechtsgrundlage (Zweckänderung Art. 6 Abs. 4 DS-GVO) zu prüfen. Wird fortan die Videoüberwachung mit dem Zweck betrieben, festzustellen, ob erneut strafrechtlich relevantes Verhalten auftritt, ist diese Videoüberwachung an den Grundsätzen der DS-GVO zu prüfen, da nun für diesen Zweck – mögliche Übergabe an Strafverfolgungs-

behörden – die Privilegierung des Art. 2 Abs. 2 Buchstabe c) DS-GVO nicht mehr greift. In diesem Falle ist die Videoüberwachung an der Rechtsgrundlage Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zu messen. Die Videoüberwachung ist danach rechtmäßig, wenn die Videoüberwachung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und das schutzwürdige Interesse der betroffenen Person das berechtigte Interesse des Verantwortlichen nicht überwiegt. Allerdings überwiegt das Interesse des Betroffenen (Straftäters) nicht das Interesse des Verantwortlichen. Erfasst die zunächst als familiäre Datenverarbeitung gedachte Videoüberwachung auch öffentliche Bereiche wie die Straße vor der Haustür, findet die DS-GVO Anwendung. Bereits mit Urteil vom 11. Dezember 2014 hat der Europäische Gerichtshof (EuGH) in der Rechtssache Ryneš (C-2012/13) entschieden, dass eine Videoüberwachung, die sich auch auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre gerichtet ist, nicht als „ausschließlich persönliche oder private Tätigkeit angesehen“ werden kann. Gleiches gilt bei der Videoüberwachung von Nachbargrundstücken, da auch hier die Videoüberwachung den ausschließlich privaten und familiären Bereich verlässt (so auch Scholz in Simitis, Kommentar zum Datenschutzrecht, 1. Auflage, Anhang zu Art 6, Rn. 49). Hier wird ebenfalls die persönliche Sphäre des Kamerabetreibers verlassen. Weiterhin stellt sich die gleiche Problematik bei Datenverarbeitungen von kamerabestückten Drohnen. Soweit Drohnen auch öffentliches Gebiet oder Grundstücke Dritter überfliegen, wird die persönliche und familiäre Sphäre verlassen und die DS-GVO findet Anwendung.

III. Keine Anwendbarkeit des Haushaltsprivilegs

Die Tätigkeiten müssen immer auf den engen Bereich des Persönlichen oder Familiären begrenzt sein. Da die Datenverarbeitung, um unter das Haushaltsprivileg zu fallen, ausschließlich persönlichen oder familiären Zwecken dienen darf, ist die DS-GVO bei gemischten Datensammlungen wie Adressbüchern, die private und geschäftliche Kontakte beinhalten, anwendbar (so auch Kühling/ Raab in Kühling / Buchner Kommentar zur Datenschutz-Grundverordnung, 2. Auflage, Art. 2, Rn. 26). Dies umfasst insbesondere auch privat und beruflich genutzte Smartphones (so auch Roßnagel in Simitis, Kommentar zum Datenschutzrecht, 1. Auflage, Art. 2, Rn. 28). Zudem darf die Verarbeitung auch keinen Zusammenhang oder Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit haben. Ebenso gelten Tätigkeiten im ehrenamtlichen Bereich, wie beispielsweise bei Sportvereinen, nicht

als rein persönliche Tätigkeit. Die Nutzung sogenannter sozialer Netzwerke und andere Online-Tätigkeiten kann nur dann unter das Haushaltsprivileg fallen, wenn sichergestellt ist, dass nur der Nutzer auf die Daten zugreifen kann. Bei der Veröffentlichung personenbezogener Daten im Internet, insbesondere im Rahmen sozialer Medien, ist entscheidend: Sollen die personenbezogenen Daten in einem sozialen Netzwerk eingestellt werden, ist bei einer durch Nutzernamen und Passwort geschützten Gruppe oder einem Forum auf einer Webseite davon auszugehen, dass dies wegen des ausschließlichen Zugriffs des persönlichen Umfelds gerade noch unter das Haushaltsprivileg fällt. Werden die Daten in diesem Nutzerbereich jedoch einem unbeschränkten Personenkreis zugänglich gemacht, beispielsweise durch die Bereitstellung der Aufnahmen auf einer frei zugänglichen Webseite, scheidet eine Annahme des Haushaltsprivilegs aus, die DS-GVO ist mithin anwendbar (so der EuGH bereits in der Lindqvist-Entscheidung – EuGH Urteil vom 6. November 2004, C-101/01, auch Leitlinien des Europäischen Datenschutzausschusses EDSA zur Videoüberwachung – Guidelines 3/2019 on processing of personal data through video devices, abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Guidelines_03_2019.pdf) .

4.18 Keine familiären Tätigkeiten trotz Verwandtschaftsverhältnis

Die Inanspruchnahme der Ausnahme familiärer Tätigkeiten ist ausgeschlossen, wenn die Datenverarbeitung mit einem Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Im Fall familienrechtlicher Streitigkeiten ist die Datenschutz-Grundverordnung anwendbar, da zur Regelung der Gewinnabschöpfung aus dem Verkauf des elterlichen Hauses ein Anwalt beauftragt wurde.

Die Datenschutz-Grundverordnung (DS-GVO) findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, so Art. 2 Abs. 2 Buchstabe c) DS-GVO. Unter diesem sogenannten Haushaltsprivileg werden häufig Datenverarbeitungen vor-

genommen, welche dennoch nach DS-GVO zu bewerten sind und für die keine Rechtsgrundlage vorliegt. So auch in folgendem Fall:
Herr Schmidt schloss mit seiner Schwester Frau Müller, deren Ehemann Herrn Müller und seinen Eltern einen Vertrag zum Grundbesitz des Wohnhauses (aus Datenschutzgründen werden hier selbstverständlich nicht die richtigen Namen genannt). In dem Vertrag zum Grundbesitz wurde unter anderem die Verfahrensweise bei einem möglichen Verkauf der Immobilie festgelegt. Die Immobilie sollte nunmehr verkauft werden. Hierfür beauftragte Herr Schmidt einen Rechtsanwalt. Im Berichtszeitraum leitete Herr Schmidt eine E-Mail des Herrn Müller an die Tochter der Eheleute Müller (Sandra) weiter. Als Anlage zu dieser E-Mail waren eine Abrechnung des Wohnhauses mit Summen zum Verkaufspreis, zu Tilgungssummen sowie Angaben zu Lebensversicherungen und Bankdaten enthalten.
Herr Müller beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Weiterleitung der E-Mail mit den sensiblen Informationen zum Immobilienverkauf an seine Tochter Sandra durch Herrn Schmidt.
Herr Schmidt trug im Rahmen der Sachverhaltsaufklärung vor, dass es sich bei der Übermittlung der E-Mail mit den Informationen zur Immobilie um eine familiäre Tätigkeit handelt und daher die DS-GVO keine Anwendung findet. Herr Schmidt übermittelte die personenbezogenen Daten an seine Nichte Sandra, weil er seinen Gewinn aus dem Verkauf des elterlichen Hauses zwischen Sandra und seiner Tochter aufteilen wollte. Der TLfDI prüfte und bewertete die Angelegenheit wie folgt:
Die Übermittlung der personenbezogenen Daten zum Immobilienverkauf an seine Nichte Sandra stellt nach Art. 4 Nr. 2 DS-GVO eine Verarbeitung personenbezogener Daten dar. Dafür ist eine Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 DS-GVO erforderlich. Eine Einwilligung der von der Datenverarbeitung betroffenen Personen lag nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO nicht vor. Da Sandra kein Vertragspartner im Vertrag über den Grundbesitz des Wohnhauses ist, kommt die Verarbeitung der personenbezogenen Daten zum Immobilienverkauf zur Vertragserfüllung nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO auch nicht in Betracht.
Eine zulässige Datenübermittlung kommt daher nur nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zur Wahrung der berechtigten Interessen des Herrn Schmidt in Betracht, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwie-

gen. Aus dem Inhalt der an seine Nichte Sandra gesandten E-Mail lässt sich nicht entnehmen, dass sie etwa einen Gewinnanteil aus dem Hausverkauf aus rechtlichen Gründen hätte erwarten können. Vielmehr entstand der Eindruck einer Rechtfertigung, aus welchen Gründen Herr Schmidt in dieser Angelegenheit einen Rechtsanwalt beauftragt hat. Die personenbezogenen Daten der Vertragspartner an seine Nichte Sandra zu übermitteln, war weder für eine etwaige Gewinnbeteiligung aus dem Verkauf des elterlichen Hauses erforderlich noch geeignet. Für die Auszahlung des Gewinnbetrages wären die Herkunft und die Vertragsbestandteile für Sandra unerheblich und auch nicht zu belegen gewesen.
Auf jeden Fall überwogen aber die schutzwürdigen Interessen der von der Datenübermittlung betroffenen Personen, unter anderem Herr Müller. Gerade weil es sich bei Sandra um die Tochter des Herrn Müller handelte, ist das Persönlichkeitsrecht der betroffenen Personen zu beachten. Jeder entscheidet im Rahmen seines Grundrechts auf informationelle Selbstbestimmung selbst, wem wann welche Informationen zur eigenen Person bekannt gegeben werden. Sandra hätte selbst die Informationen zum oben genannten Vertrag von ihren Eltern erhalten können, wenn diese sich aktiv dafür entschieden hätten.
Soweit sich Herr Schmidt darauf stützte, dass es sich bei der Datenübermittlung an seine Nichte Sandra um eine familiäre Tätigkeit im Sinne des Art. 2 Abs. 2 Buchstabe c) DS-GVO handelt, kann dieser Argumentation nicht gefolgt werden. Es ist zwar festzustellen, dass familiäre Tätigkeiten alle Tätigkeiten umfassen, die der Pflege familiärer Beziehungen und des familiären Zusammenhalts dienen. Der Begriff „familiär“ ist dennoch nicht rein familienrechtlich auszulegen. Er umfasst unabhängig von Ehe, Kindschaft und Verwandtschaft jede Beziehung, die eine vergleichbare persönliche Nähe aufweist und von der Verkehrsanschauung als familiär angesehen wird. Allerdings ist nach dem Erwägungsgrund (EG) 18 der DS-GVO die Inanspruchnahme dieser Ausnahme ausgeschlossen, wenn die Datenverarbeitung mit einem „Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird“ (Roßnagel in Simitis, DS-GVO, 1. Auflage, Art. 2, Rn. 24 ff). Die Verwaltung privaten Vermögens gehört grundsätzlich zum persönlichen Bereich, soweit sie nicht nach Form und Umfang einer geschäftlichen Tätigkeit gleicht. Geschäftlich ist jede wirtschaftliche Tätigkeit, ganz gleich ob tatsächlich Mittel fließen. Jegliche den persönlich-familiären Bereich überschreitende Nutzung führt zur Unanwendbarkeit der Ausnahme des Art. 2 Abs. 2 Buch-

stabe c) DS-GVO. Eine persönliche oder familiäre Tätigkeit ist öffentlichkeitsfeindlich (Ernst in Paal/Pauly, DS GVO/BDSG, 2 Auflage, Art. 2, Rn. 19). Im Laufe des Verfahrens wurde zur Regelung der Gewinnabschöpfung aus dem Verkauf der Immobilie ein Anwalt beauftragt. Daher ist im vorliegenden Fall nicht von einer familiären Beziehung der beteiligten Personen untereinander auszugehen. Eine Berufung auf familiäre Tätigkeiten läuft demzufolge fehl.
Im Ergebnis wurde festgestellt, dass die Übermittlung der personenbezogenen Vertragsdaten an die Nichte Sandra zur Gewinnbeteiligung aus dem Verkauf des elterlichen Hauses nicht erforderlich und danach nicht rechtmäßig war. Herr Schmidt wurde vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit entsprechend Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt. Darüber hinaus entschuldigte sich Herr Schmidt bei seiner Schwester Frau Müller und deren Ehemann Herrn Müller für die von ihm vorgenommene Datenübermittlung an seine Nichte. Gleichzeitig bat er Sandra Müller um Löschung der von ihm übermittelten Daten zum Verkauf der Immobilie.

4.19 Unterhaltsvorschussantrag – welche Daten des nicht mit den Kindern lebenden Elternteils dürfen ans Jugendamt weitergegeben werden?

Übermittelt der mit den Kindern lebende Elternteil im Rahmen einer Unterhaltsstreitigkeit erhaltene Einkommens- und Vermögensnachweise des anderen Elternteils an das Jugendamt, steht diese Übermittlung im Einklang mit der Datenschutz-Grundverordnung. Das schutzwürdige Interesse des anderen Elternteils, über die Empfänger seiner personenbezogenen Daten selbst zu entscheiden, überwiegt nicht das berechtigte Interesse des mit den Kindern lebenden Elternteils an der Übermittlung der Daten an das Jugendamt im Rahmen eines Unterhaltsvorschussantrags nach den Vorschriften des Unterhaltsvorschussgesetzes.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über eine Datenverarbeitung im Rahmen einer Familienstreitigkeit.

Die Parteien hatten sich getrennt und im Folgenden kam es zu Streitigkeiten über den zu zahlenden Unterhalt für die gemeinsamen Kinder. Der bei den Kindern verbliebene Elternteil (im folgenden familiennaher Elternteil) forderte den familienfernen Elternteil (nicht mit den Kindern lebenden: Beschwerdeführer) auf, alle Unterlagen, die zur Berechnung des Unterhalts erforderlich seien, zu übersenden. Die so erhaltenen Einkommensnachweise übermittelte der familiennahe Elternteil sodann im Rahmen eines Antrags auf Unterhaltsvorschuss an das zuständige Jugendamt. Hierrüber beschwerte sich der familienferne Elternteil beim TLfDI.
Der familiennahe Elternteil rechtfertigte die Übermittlung mit Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO), wonach die Verarbeitung rechtmäßig ist, soweit eine rechtliche Verpflichtung die Datenverarbeitung erforderlich macht. Gestützt werde die Verpflichtung zur Datenweitergabe auf § 6 Abs. 1 Unterhaltsvorschussgesetz (UVG) beziehungsweise im nächsten Schritt auf die Richtlinie zur Durchführung des Unterhaltsvorschussgesetzes, die den Antragsteller verpflichte, alle ihm vorliegenden Angaben über das Vermögen des familienfernen Elternteils dem zuständigen Jugendamt mitzuteilen.
Der TLfDI sah in Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 Buchstabe b) DS-GVO in Verbindung mit § 6 Abs. 1 UVG keine geeignete Rechtsgrundlage für die Datenübermittlung. Allerdings ist sie nicht rechtswidrig, vielmehr stellt Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO die geeignete Rechtsgrundlage für eine Übermittlung der Daten an das Jugendamt dar.
Der TLfDI stellte zunächst fest, dass die Einkommensnachweise personenbezogene Daten nach Art. 4 Nr. 1 DS-GVO enthalten und die Weitergabe an Dritte, hier das Jugendamt, eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DS-GVO darstellt. In der Überlassung der Einkommensnachweise zur Berechnung von Unterhaltsansprüchen an den familiennahen Elternteil lag keine Einwilligung zur Übermittlung dieser Daten an das Jugendamt nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO.
Unter den Voraussetzungen des § 1 Abs. 1 UVG konnte der familiennahe Elternteil Unterhaltsvorschuss beim Jugendamt beantragen. Grundsätzliche Voraussetzung ist, dass der Unterhalt nicht / nicht in voller Höhe seitens des familienfernen Elternteils gezahlt wird. Der Anspruch auf Unterhalt geht sodann nach § 7 UVG auf das Land über und dieses setzt den Anspruch gegenüber dem familienfernen Eltern-

teil durch. Daher ist der familienferne Elternteil entsprechend § 6 Abs. 4 UVG verpflichtet, gegenüber dem Jugendamt Angaben über die Höhe seines Einkommens / Vermögens und sonstige unterhaltsbegründender Tatsachen zu machen.
Nach Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 DS-GVO ist die Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Zwar stellt das Unterhaltsvorschussgesetz eine geeignete Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 DS-GVO dar. Jedoch müssen die Regelungen über die Datenverarbeitungen so klar und präzise die Verarbeitungsvoraussetzungen beschreiben, dass die Verarbeitung für die Rechtsunterworfenen klar erkennbar ist (Kühling/Buchner, Kommentar Datenschutzgrundverordnung, Art. 6 Rn. 84). Auch muss gemäß Art. 6 Abs. 3 Satz 2 DS-GVO der Zweck der Verarbeitung gesetzlich festgelegt sein. Eine Auskunftspflicht über die Einkommens- und Vermögensverhältnisse des familienfernen Elternteils und mithin die Übermittlung der Einkommensnachweise an das Jugendamt des antragstellenden Elternteils ergibt sich nicht direkt aus den Vorschriften des UVG. Entsprechend § 6 Abs. 1 und Abs. 4 UVG ergibt sich lediglich eine direkte Auskunftspflicht des familienfernen Elternteils gegenüber dem Jugendamt.
Da zum einen als Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 Buchstabe c), Abs. 3 DS-GVO ausschließlich Gesetze im materiellen Sinne herangezogen werden dürfen und zum anderen die Regelungen zur Datenverarbeitung klar, präzise und vorhersehbar in der Rechtsvorschrift niedergelegt sein müssen, konnte die Richtlinie zur Durchführung des Unterhaltsvorschussgesetzes nicht herangezogen werden. Beide Voraussetzungen erfüllt die Richtlinie nämlich nicht.
Die Datenverarbeitung war jedoch nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO rechtmäßig. Danach ist die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern.
Um das Einkommen einer Familie mit Kindern zu sichern, steht es im berechtigten Interesse des familiennahen Elternteils, Unterhaltsverpflichtungen zügig zu klären und gegebenenfalls schnellstmöglich einen Unterhaltsvorschuss zu beantragen, um Unterhalt für die Kinder zu erlangen. Im Rahmen eines Unterhaltsvorschussantrages sind bereits Angaben zum Vermögen des familienfremden Elternteils zu ma-

chen. Auch die Richtlinie zur Durchführung des Unterhaltsvorschussgesetzes sieht Mitwirkungsrechte des antragstellenden Elternteils nach § 1 Abs. 3 UVG vor, wonach er zu umfassenden Auskünften zu den Einkommens- und Vermögensverhältnissen des familienfernen Elternteils (Ziff. 1.10.1. und 6.2 der Richtlinie) verpflichtet ist.
Das schutzwürdige Interesse des familienfernen Elternteils als betroffene Person überwog nicht. Zwar bestand ein schutzwürdiges Interesse daran, selbst zu entscheiden, wer sensible Daten wie Einkommens- und Vermögensnachweise erhält. Hier musste berücksichtigt werden, dass der Unterhaltsanspruch der Kinder auf das Land übergegangen war (§ 7 UVG). Diesen Anspruch konnte sodann das Jugendamt gegenüber dem familienfernen Elternteil durchsetzen. Insoweit war dieser nach § 6 Abs. 1 und 4 UVG verpflichtet, gegenüber dem Jugendamt Auskunft über seine Vermögens- und Einkommensverhältnisse zu geben und alle relevanten Daten zu übermitteln.
Im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO war hier entscheidend, ob die betroffene Person zum Zeitpunkt der Datenerhebung vernünftigerweise absehen konnte, dass eine Datenverarbeitung stattfinden wird. Im Rahmen von Unterhaltsstreitigkeiten ist zu erwarten, dass das Jugendamt zur Klärung offener Fragen einbezogen wird. Auch kann der Betroffene erwarten, sofern er als familienfernes Elternteil selbst keinen Unterhalt zahlt und für die Unterhaltspflicht das Land im Rahmen eines Unterhaltsvorschusses eintreten muss, dass auch Angaben zu seinem Vermögen und Einkommen gegenüber dem Jugendamt getätigt werden.
Im berechtigten Interesse des familiennahen Elternteils als Verantwortlichem lag es, vollumfänglich alle notwendigen Angaben gegenüber dem Jugendamt zu tätigen, um schnellstmöglich einen Unterhaltsvorschuss zu erhalten. Zudem war zu berücksichtigen, dass nicht ein Dritter die Daten erhält, sondern die Stelle, der der familienferne Elternteil selbst gegenüber auskunftspflichtig war. Im Ergebnis fiel die Interessenabwägung zugunsten des Verantwortlichen aus. Dem Beschwerdeführer und dem Verantwortlichen wurde mitgeteilt, dass die Datenweitergabe mithin nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO datenschutzrechtlich rechtmäßig war.

4.20 Sind Ortschroniken nach Inkrafttreten der DS-GVO noch zulässig?

Werden Ortschroniken mit personenbezogenen Daten erstellt und veröffentlicht, gelten die Vorschriften der Datenschutz-Grundverordnung (DS-GVO). In der Regel ist für die Veröffentlichung von Fotos, auf denen Personen abgebildet sind, und für die Namensnennung eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO erforderlich.

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, was bei der Erstellung einer Ortschronik nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) alles zu beachten sei. Er beschrieb seine Tätigkeit folgendermaßen: Er wolle möglichst alle Ereignisse des Ortes festhalten und hierzu auch Fotos und Namen von Bewohnern verwenden. Hierzu fehle ihm fast immer die Einwilligung der Betroffenen, die bei lang zurückliegenden Ereignissen und alten Fotos auch kaum mehr einholbar sei. Er sei nicht journalistisch tätig. Zudem möchte er nun zu der bereits erstellten Ortschronik eine Ausstellung in seinem Ort organisieren und fragte beim TLfDI, ob dies überhaupt zulässig sei.
Der TLfDI hat zunächst die Anwendbarkeit der DS-GVO bejaht. Für die Verarbeitung personenbezogener Daten im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten, bei denen jeglicher Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit fehlt, ist gemäß Art. 2 Abs. 2 DSGVO die Datenschutz-Grundverordnung nicht anwendbar (sog. Haushaltsprivileg). Dieses Haushaltsprivileg greift nicht, soweit Chroniken veröffentlicht werden sollen oder nur ein Teil der Chronik im Rahmen einer Ausstellung öffentlich gezeigt werden soll, da dann der ausschließlich persönliche und familiäre Bereich überschritten wird. Jedoch ist die DS-GVO nicht anwendbar, soweit Verstorbene auf Fotos gezeigt oder namentlich genannt werden, da die DS-GVO nach Art. 1 Abs. 1 DS-GVO nur dem Schutz natürlicher, also lebender Personen dient (Erwägungsgrund 27 zur DS-GVO).
Bei der Veröffentlichung von Fotos muss für jedes einzelne Foto ermittelt werden, ob eine Veröffentlichung im Sinne der DS-GVO zulässig ist oder nicht.
Die Veröffentlichung von Fotos mit Personenbezug stellt eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DS-GVO dar.

Gleiches gilt für die Veröffentlichung von Personennamen im Kontext bestimmter Ereignisse.
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. Die DS-GVO enthält somit ein Verbot mit Erlaubnisvorbehalt.
Folgendes ist zu beachten:
Bei der Veröffentlichung von Fotos, auf denen Dorfbewohner zu sehen sind, ist zu unterscheiden, ob die abgebildete Person im Vordergrund steht, dann ist grundsätzlich eine Einwilligung des Abgebildeten entsprechend Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO für die Veröffentlichung einzuholen. Die Voraussetzungen einer rechtmäßigen Einwilligung im Sinne des Art. 7 DS-GVO und die Informationspflichten nach Art. 13 Abs. 1 DS-GVO sind dabei zu beachten. Handelt es sich bei der abgebildeten Person um eine Person des öffentlichen Lebens, galt bisher, dass nach § 23 Kunsturhebergesetz (KUG) eine Einwilligung entbehrlich ist, soweit es sich um Fotos von Personen aus dem Bereich der Zeitgeschichte handelt. Nun gelten §§ 22, 23 KUG nach Inkrafttreten der DS-GVO nicht mehr unmittelbar, da die DS-GVO als europäische Verordnung unmittelbar gilt und ihr ein Anwendungsvorrang zusteht. Im Rahmen der Wertung der zulässigen Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) und f) DS-GVO fließen die bisherigen Grundsätze des KUG jedoch ein (so auch LG Frankfurt, Urteil vom 26. September 2019, 2-03 O 402/18, dass die Anwendbarkeit der Grundsätze der §§ 22, 23 KUG für Art. 6 Abs. 1 Satz 1 Buchstabe f), 85 Abs. 2 DS-GVO für weiterhin anwendbar erklärt). Daher ist bei Persönlichkeiten der Zeitgeschichte, wie Lokalpolitikern, Künstlern, Schauspielern, Sängern, Schriftstellern und Sportlern, auch weiterhin davon auszugehen, dass für die Veröffentlichung von Fotos dieser Personen im zeitgeschichtlichen Rahmen keine Einwilligung erforderlich ist. Zur Zeitgeschichte zählt das gesamte politische, soziale, wirtschaftliche und kulturelle Leben und was Gegenstand der Aufmerksamkeit oder Anteilnahme der Öffentlichkeit ist. Anders sieht es für die Veröffentlichung von Fotos von Personen der Zeitgeschichte im privaten Kontext (Fotos der Lebenspartner, Kinder) aus. Hier ist die Privatsphäre der Person zu berücksichtigen und die öffentliche Relevanz in der Regel nicht gegeben. Mithin bedarf es für die Veröffentlichung dieser Fotos grundsätzlich einer Einwilligung. Dabei muss immer und für jedes einzelne Foto se-

parat entschieden werden, ob es sich um einen Kontext handelt, bei dem sich der Fotografierte im Privaten zeigt, oder ob das Informationsinteresse der Allgemeinheit überwiegt, da die Aufnahme den Kontext der Privatsphäre verlässt. Als Richtschnur gilt: Je unbekannter eine Persönlichkeit ist und je weniger sie öffentlich von sich privat preisgegeben hat, desto eher bedarf es einer Einwilligung.
Davon zu unterscheiden ist die Verwertung von Aufnahmen, auf denen sich eine Vielzahl von Personen befindet, zumeist zusätzlich als sogenanntes Beiwerk oder im Rahmen von Übersichtsaufnahmen, zum Beispiel Zuschauerränge bei Sportveranstaltungen, Publikumsaufnahmen im Hintergrund künstlerischer Darbietungen. Bei übersichtsartigen Bildaufnahmen, auf denen viele Personen zu sehen sind, ist die Einholung einer Einwilligung oder die Information der Abgelichteten über ihre Rechte für die Fotografen nahezu unmöglich Daher fließen bei der Bewertung, inwieweit eine Einwilligung notwendig ist, ebenfalls die Grundsätze des KUG ein. Ob die Person „Beiwerk“ ist, lässt sich gut anhand der Frage prüfen: Kann die Person auch weggelassen werden, ohne dass sich der Gegenstand und Charakter des Bildes verändern? Ist die abgebildete Person dagegen der Blickfang des Bildes, dann ist die Person kein Beiwerk und eine Einwilligung ist erforderlich. Auch hier ist eine Einzelfallbetrachtung notwendig.

Weitere Informationen hierzu / 18, Urt. V. finden Sie auf der Homepage des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/umgang_mit_fotoaufnahmen_im_rahmen_der_oeffentlichkeitsarbeit_von_vereinen_.pdf
Bei der Veröffentlichung von Namen sollte grundsätzlich darauf abgestellt werden, inwieweit es sich bei der genannten Person um eine Person handelt, die im Rahmen ihrer Amtsausübung dargestellt wird, wie beispielsweise Bürgermeister oder Vereinsvorsitzende. Je eher die Person als Privatperson handelte und in diesem Zusammenhang genannt wird, desto eher ist eine Einwilligung vor Veröffentlichung des Namens notwendig. Die zuvor genannten Grundsätze zur Veröffentlichung von Fotos von Personen der Zeitgeschichte können hier herangezogen werden.
Sie gelten unabhängig davon, ob die Erstellung der Ortschronik durch eine Privatperson oder durch einen Verein vorgenommen wird. Entscheidend ist allein, ob die Chronik veröffentlicht wird und damit der

rein familiäre und persönliche Bereich entsprechend Art. 2 Abs. 2 DS-GVO verlassen wird. Das zuvor gesagte gilt sowohl für Veröffentlichung in Buchform, im Internet oder im Rahmen einer Ausstellung. Dabei muss die Einwilligung, soweit nach dem oben gesagten eine Einwilligung erforderlich ist, für jede Art der Veröffentlichung (Buchform, Internet, Ausstellung) eingeholt werden.

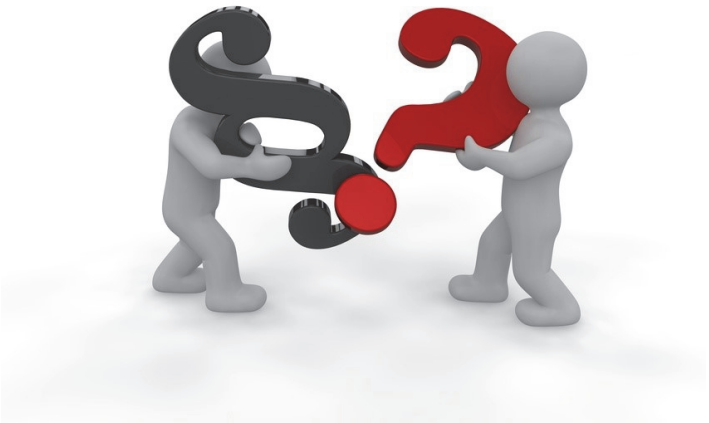
4.21 Augen auf bei der Rechtsanwendung – Unrechtmäßige Mandantenakquise einer Rechtsanwaltskanzlei aufgrund rechtmäßig erhaltener Gerichtsakten

Anwaltskanzleien erhalten im Rahmen von Akteneinsichten bei Gericht immer auch personenbezogene Daten zur Kenntnis. Diese dürfen nur für das Mandat beziehungsweise die Mandate genutzt werden, im Rahmen deren Durchführung auch Einsicht genommen wurde. Eine nicht mandatsbezogene Nutzung (zum Beispiel zu Akquisezwecken) stellt eine unzulässige Zweckänderung dar, die bußgeldbewehrt ist. Ein solcher Datenschutzverstoß kann nach DS-GVO mit einer Höhe von bis zu 20.000.000,00 Euro geahndet werden.

Im Rahmen einer Beschwerde gegen eine thüringische Anwaltskanzlei wurde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wegen der Schwere des Verstoßes ein Ordnungswidrigkeitenverfahren eröffnet.
Eine Fondsgesellschaft hatte aufgrund Zahlungsschwierigkeiten Insolvenz angemeldet. Die geschädigten Anleger der betreffenden Gesellschaft wurden durch den vom Gericht bestellten Insolvenzverwalter, über das Verfahren informiert. Im Rahmen der Mandatsbearbeitung einzelner Anleger der Fondsgesellschaft beantragte eine thüringische Rechtsanwaltskanzlei Akteneinsicht beim zuständigen Insolvenzgericht. Die Kanzlei erlangte so Kenntnis über 4.000 ebenfalls geschädigte Anleger.
In der Folge wurden durch die Kanzlei diese ebenfalls geschädigten Anleger angeschrieben, mit dem Hinweis, dass eine Mandatierung der Kanzlei möglich sei. Dem Schreiben waren vorausgefüllte Vollmachten und Mandantenstammblätter, welche durch die geschädigten Anleger lediglich unterschrieben und zurückgeschickt werden mussten, beigelegt. In den betreffenden Schreiben wurde den geschädigten Anlegern weiterhin suggeriert, dass sie ihr eingelegtes Geld wenigstens teilweise wiedererhalten würden.

Da sich der Datenschutzverstoß noch vor dem Wirksamwerden der Datenschutz-Grundverordnung ereignete, war dieser nach dem Bundesdatenschutzgesetz in der alten Fassung vom 14. August 2009 (BDSG a. F.) zu bewerten gewesen. Nach § 28 Abs. 5 Satz 1 BDSG a. F darf die Rechtsanwaltskanzlei die Anlegerdaten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt worden sind. Der Zweck der Datenübermittlung vom Insolvenzgericht an die Rechtsanwaltskanzlei entsprach allein der Mandatsbearbeitung. Eine gemäß § 299 Zivilprozessordnung (ZPO) beantragte Akteneinsicht wurde aufgrund des bestehenden Mandatsverhältnisses erteilt. Eine Notwendigkeit der Mandatsakquise für die bestehende Mandatsbearbeitung bestand nicht. Die Rechtsanwaltskanzlei nutzte die personenbezogenen Anlegerdaten, um die Anleger für die eigene Kanzlei zu werben. Damit überschritt die Rechtsanwaltskanzlei ihre Befugnisse für die Bearbeitung des Insolvenzverfahrens nach § 28 Abs. 5 Satz 2 BDSG a. F. Danach ist eine Verarbeitung oder Nutzung für andere Zwecke für nicht-öffentliche Stellen nur nach den Voraussetzungen des § 28 Absätze 2 und 3 BDSG a. F. erlaubt. Diese Voraussetzungen lagen für die Rechtsanwaltskanzlei nicht vor, da in jedem Fall die schutzwürdigen Interessen der Anleger einer zweckändernden Nutzung überwogen. Somit war der Rechtsanwaltskanzlei durchaus bewusst, dass die Verarbeitung der personenbezogenen Daten, welche sie im Rahmen der Mandatsbearbeitung nach § 299 ZPO einsehen und gebrauchen durfte, unrechtmäßig war.
Gemäß § 43 Abs. 1 Nr. 4 BDSG a. F. handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 28 Abs. 5 Satz 2 BDSG a. F. personenbezogene Daten übermittelt oder nutzt. Die Anwaltskanzlei hat als Dritter (Empfänger der Akteneinsicht) die Daten im Rahmen der Mandatsbearbeitung vom Gericht rechtmäßig erhalten. Der Zweck entsprach allein der Mandatsbearbeitung, nicht der Werbung um weitere Mandatierungen. Eine Nutzung der aufgrund der Akteneinsicht zur Verfügung gestellten personenbezogenen Daten für Werbezwecke ist vom ursprünglichen Mandatsverhältnis nicht gedeckt und damit nicht zweckgerichtet.
Dieser Datenschutzverstoß wurde durch den TLfDI mit einem Bußgeld in Höhe von über 10.000,00 Euro geahndet.

5. Entschließungen und Beschlüsse



© ilro - Paragraph und Fragezeichen - fotolia.com

5.1 Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!

Entschließung
der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 3. April 2019[1] in Neustadt a. d. Weinstraße

Unternehmen haften im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem

[1] Gegen die Stimmen von Bayern und Baden-Württemberg

Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend daraufhin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse“), sind ausgenommen.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unternehmen generell im deutschen Recht so zu ändern, dass „die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden“. Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

5.2 Hambacher Erklärung zur Künstlichen Intelligenz Sieben datenschutzrechtliche Anforderungen

Entschließung
der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 3. April 2019 Hambacher Schloss

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ [...].“[2]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

[2] BT-Drs. 19/1982 zu 1., Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018;).

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für

die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u. a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung. Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DS-GVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und

Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutzaufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

5.3 Keine Abschaffung der Datenschutzbeauftragten

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
Stand: 23. April 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.
Nach § 38 Bundesdatenschutzgesetz müssen z. B. Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.
Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutz-Grundverordnung bewährt.
Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.
Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

5.4 Digitalisierung der Verwaltung – datenschutzkonform und bürgerfreundlich gestalten!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 12. September 2019

Die Bundesregierung will die in der Verwaltung geführten Register modernisieren und plant in diesem Zusammenhang einen einfacheren Zugriff auf dort gespeicherte personenbezogene Daten. Nach Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) darf dieses Vorhaben nicht zur Einführung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren führen. Vielmehr muss der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten, Priorität haben. Ebenso wichtig ist es, den Bürgerinnen und Bürgern die besseren Dienstleistungen verbunden mit einer deutlich höheren Transparenz anzubieten.

Bundesregierung nimmt Modernisierung der Register in Angriff

Die Bundesregierung hat mit dem Onlinezugangsgesetz ein umfangreiches Digitalisierungsprogramm für die Verwaltung in Deutschland gestartet. Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten. Es sollen Nutzerkonten bereitgestellt werden, über die sich Nutzende für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.
In diesem Zusammenhang hat sich der Nationale Normenkontrollrat (NKR) für eine Modernisierung der deutschen Registerlandschaft ausgesprochen und empfohlen, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only"-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen und ein „Datencockpit" einzurichten, bei dem die Bürgerinnen und Bürger alle staatlichen Datenflüsse im Auge haben können. Die Einführung

solcher Identifikationsnummern für Personen wird aktuell unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) von der Bundesregierung verfolgt. Der IT-Planungsrat hat in seiner 28. Sitzung am 12. März 2019 den vom BMI vorgelegten „Leitlinien für eine Modernisierung der Registerlandschaft“ zugestimmt sowie den „Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung“ zur Kenntnis genommen und das angestrebte Vorhaben begrüßt.

Datenschutzfreundliche und transparente Gestaltung für Bürgerinnen und Bürger

Bereits die Schaffung einheitlicher und verwaltungsübergreifender Personenkennzeichen bzw. Identifikatoren und einer entsprechenden Infrastruktur zum Datenaustausch bergen die Gefahr, dass personenbezogene Daten in großem Maße leicht zusammengetragen, verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden könnten. Die Datenschutzkonferenz weist darauf hin, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat gefährdet das Persönlichkeitsrecht, da sie bei den Menschen zu einer vorauseilenden Anpassung ihres Verhaltens führen kann. Auch die Grundsätze der europäischen Datenschutz-Grundverordnung und deren Regelungen zur datenschutzgerechten Gestaltung setzen einheitlichen und verwaltungsübergreifenden Personenkennzeichen enge Grenzen und verlangen geeignete Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen.
Insbesondere im Hinblick auf die geplante Verwendung modernisierter Register für zukünftige Zensus-Erhebungen und geplante/modernisierte Zugriffsrechte der Sicherheitsbehörden bedarf es eines besonderen Schutzes der betroffenen Personen. Den hohen Risiken für das Recht auf informationelle Selbstbestimmung muss in einem umfassenden regulatorischen, vor allem aber technischen und organisatorischen Konzept begegnet werden. Nur so können die vom deutschen und europäischen Verfassungsrecht geforderten Garantien gewahrt werden.

Die Modernisierung der Register muss zwingend von Beginn an auch dafür genutzt werden, den Bürgerinnen und Bürgern die Nutzung der im Online-Zugangsgesetz vorgesehenen Dienstleistungen durch Nutzung einmal hinterlegter Daten zu erleichtern. Von besonderer Bedeutung ist es darüber hinaus, den Bürgerinnen und Bürgern ein im Vergleich zur gegenwärtigen Situation deutlich höheres Maß an Transparenz zu gewährleisten. Ein „Datencockpit“, wie es der NKR bereits vorgeschlagen hat, muss es den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welches Register welche Daten über sie vorhält, welche Behörden darauf zugegriffen haben und mit welchen anderen Daten diese verknüpft wurden. Gleichzeitig muss gewährleistet sein, dass ausschließlich den betroffenen Bürgerinnen und Bürgern der Zugriff möglich ist. Auf dieser Grundlage muss die Digitalisierung der Verwaltung dazu genutzt werden, das informationelle Machtgefälle zwischen Staat und Bürgerinnen und Bürgern weitgehend aufzuheben und ihnen die Inanspruchnahme ihrer Rechte deutlich zu erleichtern.
Dazu muss nach Auffassung der Datenschutzkonferenz die dezentrale Registerstruktur erhalten bleiben. Die Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern lehnt die Datenschutzkonferenz ab. Sie fordert alternative Methoden zur eindeutigen Identifizierung. Neben Abgleichen über den jeweiligen Datensatz des Registers kämen dafür allenfalls sektorspezifische Personenkennziffern in Betracht, die eine eindeutige Identifizierung erlauben, einseitigen staatlichen Abgleich von Daten verhindern, ein Höchstmaß an Transparenz beispielsweise durch ein Datencockpit ermöglichen, das Risiko von Missbrauch und Kompromittierung verringern und die Eindeutigkeit von Registern gewährleisten.

5.5 Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 6. November 2019

Auf der Grundlage der Hambacher Erklärung vom 3. April 2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder(DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.
Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.
Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der DS-GVO formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der

betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.
Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

5.6 Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 6. November 2019

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutz-Grundverordnung flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.
In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.
Der Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen, unabhängig von ihrer Größe, aufgrund der Datenschutz-Grundverordnung verpflichtet.
Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem

Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

5.7 Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 6. November 2019

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking- und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.
So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking- und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie z. B. körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.
Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.
Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls

sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.
Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

- Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins – keinen eigenen Zugriff auf die weitergeleiteten Daten haben.
- Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Art. 9 Abs. 1, 2 Buchst. a Datenschutz-Grundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.
- Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.
- Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking- oder Analyse-

Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

5.8 Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 6. November 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.
Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.
Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierender Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Auswei-

tung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.
Angesichts einer fehlenden Rechtsgrundlage sieht die DSK in der geschilderten exzessiven Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung. Die DSK fordert die Polizeibehörden und Staatsanwaltschaften auf, die umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme für Zwecke der Strafverfolgung zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.
Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen einen Eingriff von erheblichem Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

5.9 Informationen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden zu Datenübermittlungen aus Deutschland in das Vereinigte Königreich Großbritannien und Nordirland ab dem 30. März 2019

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 8. März 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist Unternehmen, Behörden und andere Institutionen in Deutschland mit den folgenden Informationen auf die Rechtslage bei einem Austritt („Brexit“) des Vereinigten Königreichs Großbritannien und Nordirland (im Folgenden: VK) aus der Europäischen Union (EU) hin. Möglich sind zwei Szenarien:

1. Geregelter Austritt

Für den Fall eines geregelten Austritts („Deal-Brexit“) gilt nach den Vorgaben des vorliegenden Entwurfs eines Austrittsabkommens[3] zwischen der EU und dem VK die Datenschutz-Grundverordnung (DS-GVO) weiter. Das Abkommen sieht nämlich einen Übergangszeitraum vom 30. März 2019 bis Ende 2020 vor (Art. 126). Während dieser Zeit ist das EU-Recht, also auch die DS-GVO mit ihren Vorgaben für Datenverarbeitungen, nach wie vor auch im VK anzuwenden (Art. 127), so als wäre das Land weiterhin ein EU-Mitgliedstaat und kein Drittland im Sinne der DS-GVO.
Eine Verlängerung des Übergangszeitraums um ein bzw. zwei Jahre ist einmalig und vor dem 1. Juli 2020 möglich (Art. 132).
Während des Übergangszeitraums dürfen personenbezogene Daten in das VK unter denselben Voraussetzungen wie bisher übermittelt werden.

[3] ABl. EU vom 19. Februar 2019, C 66 I, S. 1 ff. (198Seiten), abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC%3A2019%3A066I%3ATOC

2. Ungeregelter Austritt

Für den Fall eines ungeregelten Austritts („No-Deal-Brexit“) wird das VK zu einem Drittland im Sinne der DS-GVO. Verantwortliche, die personenbezogene Daten an Partner im VK übermitteln wollen, müssen ab dem 30. März 2019 ihre Datenübermittlungen mit den besonderen Maßnahmen nach Kapitel V DS-GVO absichern. Die DSK verweist nachdrücklich auf die vom Europäischen Datenschutzausschuss (EDSA) veröffentlichte Information[4], die von allen datenübermittelnden Stellen unbedingt zu beachten ist.
Eine inoffizielle deutsche Arbeitsübersetzung[5] ist ebenfalls verfügbar. Im Wesentlichen ist demnach Folgendes zu tun:

Bei einer Datenübermittlung in das Drittland VK sollten die Verantwortlichen

1. feststellen, welche Verarbeitungen eine Übermittlung personenbezogener Daten in das Drittland VK mit sich bringen,
2. das geeignete **Datentransfer-Instrument** für die jeweilige Situation festlegen,
3. das gewählte **Datentransfer-Instrument** so umsetzen, dass es für den 30. März 2019 bereit ist,
4. in der internen Dokumentation vermerken, dass Übermittlungen in das Drittland VK erfolgen werden und
5. die Datenschutzerklärung zur Information der betroffenen Personen entsprechend aktualisieren.

Konkretisierend zu den unter Schritt 4 und 5 genannten sind insbesondere folgende Maßnahmen vorzusehen:

a) Im **Informationsblatt zur Datenverarbeitung** und in der **Datenschutzerklärung** einer Webseite ist über die Datenübermittlung in das Drittland VK und über die verwendeten geeigneten Datenschutzgarantien zu informieren (Art. 13 Abs. 1 lit. f bzw. Art. 14 Abs. 1 lit. f DS-GVO).

[4] https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/SonstigePapiere/EDSA_Info_NoDealBrexit.html?nn=5217120

[5] https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/SonstigePapiere/EDSA_Info_NoDealBrexit_Arbeits%C3%BCbersetzung.html?nn=5217120

b) Wenn eine betroffene Person von ihrem **Auskunftsrecht** Gebrauch macht, ist sie auch über die Datenübermittlung in das Drittland VK und die verwendeten geeigneten Datenschutzgarantien zu informieren (Art. 15 Abs. 1 lit. c, Abs. 2 DS-GVO).
c) Im **Verzeichnis von Verarbeitungstätigkeiten** sind Datenübermittlungen in das Drittland VK als solche zu bezeichnen und die weiteren in diesem Zusammenhang geforderten Angaben zu machen (Art. 30 Abs. 1 lit. d und lit. e DS-GVO bzw. Art. 30 Abs. 2 lit. c DS-GVO).

Die DSK weist darauf hin, dass Verantwortliche, die personenbezogene Daten ohne die **nach Kapitel V DS-GVO notwendigen Sicherheiten** in das VK übermitteln, rechtswidrig handeln. Die Aufsichtsbehörden könnten dann Datenübermittlungen per Anordnung aussetzen (Art. 58 Abs. 2 lit. j DS-GVO) und Geldbußen verhängen (Art. 83 Abs. 5 lit. c DS-GVO).

5.10 Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit[6]
Stand: 1. April 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich am 5. September 2018 zu dem (Weiter-)Betrieb von Facebook-Fanpages nach dem Urteil des EuGH vom 5. Juni 2018 geäußert. In ihrem Beschluss hat die Konferenz deutlich gemacht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25, 32 DSGVO.
Am 11. September 2018 veröffentlichte Facebook eine sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“. Diese von Facebook veröffentlichte „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO. Insbesondere steht es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten" einräumen lassen will. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen. Vor diesem Hintergrund bekräftigt die Konferenz erneut die Rechenschaftspflicht der Fanpage-Betreiber (unabhängig von dem Grad der Verantwortlichkeit) und stellt fest:

[6] Unter Enthaltung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

1. Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführen, sondern durch andere gemeinsam mit ihnen Verantwortlichen durchführen lassen.
2. Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, sind Verantwortliche nicht in der Lage, zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestehen Zweifel, geht dies zulasten der Verantwortlichen, die es in der Hand haben, solche Verarbeitungen zu unterlassen. Der EuGH führt hierzu aus: „Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.“ (EuGH, C-210/16, Rn. 40).
3. Im Hinblick auf die Ausführungen zur „Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche“ sowie zur federführenden Aufsichtsbehörde (Punkt 4 in der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“) weist die Konferenz darauf hin, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für Fanpage-Betreiber nach der DSGVO richtet. Nach Art. 55 ff. DSGVO sind die Aufsichtsbehörden für Verantwortliche (wie z. B. Fanpage-Betreiber) in ihrem Hoheitsgebiet zuständig. Dies gilt unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Kohärenzmechanismen.

Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

5.11 Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10

Auftrag
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Datenschutzrisiken moderner Betriebssysteme wurden bereits mehrfach in der DSK beraten. Die 90. DSK hat im Herbst 2015 die Entschließung zu Cloud-unterstützten Betriebssystemen verabschiedet.
Im Jahr 2017 hat das LDA Bayern auf Grundlage der alten Rechtslage des BDSG a. F. einen Prüfbericht zu Windows 10 im Unternehmensumfeld veröffentlicht. Dabei wurde unter anderem die Frage formuliert, „ob Microsoft auf die Kritik der Nutzer und anderer europäischer Datenschutzbehörden, die Windows 10 Home und Professional prüfen, reagiert und bei der Fortentwicklung von Windows 10 datenschutzrechtliche Verbesserungen vorsehen wird".
Auch das BSI hat sich im November 2018 intensiv mit Sicherheitsmängeln von Windows 10 befasst (BSI-Studie SiSyPHuS). Ein Schwerpunkt der Untersuchungen betraf die Analyse der Telemetrie Komponenten. Dabei kommt das BSI zum Ergebnis, dass sich selbst in der höchsten Sicherheitsstufe (Telemetrie-Level Security) nicht alle Datenübertragungen an Microsoft unterbinden lassen. Die SiSyPHuS-Win10-Studie des BSI adressieren dabei auch datenschutzrechtliche Risiken.
Die Marktverbreitung der Windows 10 Versionsfamilie ist inzwischen weit fortgeschritten. Im Konsumersektor, in der gewerblichen Wirtschaft sowie auch in weiten Teilen der öffentlichen Verwaltungen von Bund, Ländern und Kommunen – letztere begünstigt durch Rahmenverträge, Architektur- und Beschaffungsentscheidungen (insb. Rahmenvertragsverhandlungen 2018 des Bundes) – sind die verschiedenen Windows-10-Versionen ausgerollt worden. Zahlreiche weitere Migrationen dürften in den Jahren 2019 und 2020 im professionellen Einsatz erfolgen.
Aus technischer Sicht unterscheiden sich sowohl die Betriebssystemarchitektur als auch die Release Strategie von Windows 10 sehr deutlich von den Vorgängerprodukten. Aus datenschutzrechtlicher Sicht ist dabei auf die folgenden Aspekte ein besonderes Augenmerk zu legen:

- Windows 10 ist nicht mehr ein reines Betriebssystem sondern eine „Systemumgebung“, die neben dem eigentlichen Betriebssystem eine Vielzahl von zusätzlichen Funktionalitäten enthält. Diese können zwar individuell konfiguriert werden, wobei bei einer Standardinstallation je nach eingesetzter Produktversion nicht die datenschutzfreundlichste Voreinstellung vorhanden ist. Ob dabei das Prinzip „Data Protection by Default“ verletzt wird, ist in jedem Fall zu prüfen.
- Jedes Update (insbesondere Funktionsupdates) kann dazu führen, dass Konfigurationseinstellungen verändert werden und sich der Funktionsumfang ändert. Dies führt dazu, dass ein „neues“ Produkt vorliegt, dessen Einsatz erneut auf die datenschutzrechtliche Zulässigkeit geprüft werden muss.
- Die Datenübermittlung von Windows 10 an Microsoft kann durch alleinige Einstellungen in Windows 10 nicht vollständig unterbunden werden. Da die Übertragung verschlüsselt an Microsoft erfolgt, ist nicht abschließend festzustellen, ob und wenn ja, welche personenbezogenen Daten an Microsoft übermittelt werden.

Die Datenschutzgrundverordnung (DS-GVO) verlangt von Verantwortlichen beim Einsatz von Windows 10, die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen. Dies bedeutet für die Verantwortlichen derzeit einen erheblichen Aufwand. Er ließe sich minimieren, wenn Microsoft den Verantwortlichen einfache Möglichkeiten insbesondere zur permanenten Deaktivierung aller Datenübermittlungen bereitstellen würde.

Die DSK hat sich entschlossen, dem Arbeitskreis Technik den Auftrag zu erteilen, eine datenschutzrechtliche Positionierung zum Einsatz von Windows 10 zu erarbeiten und diese zur Grundlage eines weitergehenden, vom LDA Bayern zu koordinierenden Dialoges mit Microsoft zu datenschutzrechtlichen Fragestellungen zum Produkt Windows 10 zu machen.

5.12 Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO

Beschluss
der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 3. April 2019

Der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ wird in Erwägungsgrund 33 erwähnt, aber in der Datenschutz-Grundverordnung (DSGVO) nicht näher definiert. Er steht in einem engen inhaltlichen Zusammenhang mit der Zweckbestimmung, wie sie bei der Erteilung von Einwilligungen auszugestalten ist. Nach Art. 4 Nr. 11 DSGVO ist eine Einwilligung stets für den „bestimmten Fall“, in informierter Weise und unmissverständlich abzugeben. Das Erfordernis des „bestimmten Falls“ konkretisiert den Grundsatz der Zweckbindung im Sinne des Art. 5 Abs. 1 Buchst. b DSGVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke zu erheben sind.
In ihrem Arbeitspapier 259 rev 01, S. 33, weist die Artikel-29-Datenschutz-Gruppe überdies darauf hin, dass deswegen der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ von dem weit zu verstehenden Begriff der wissenschaftlichen Forschung in Art. 89 DSGVO zu unterscheiden ist. Dort geht es um den Anwendungsbereich der wissenschaftlichen Forschung, nicht um die Zweckbindung im Rahmen einer konkreten Datenverarbeitung. Demgegenüber ist der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ enger zu verstehen.
Daraus folgt: Nur wenn das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt (vgl. Erwägungsgrund 33, Satz 1), kann beispielsweise der Ansatz der breiten Einwilligung (broad consent) zum Tragen kommen. Bei der einer Datenerhebung zeitlich vorgelagerten Einwilligung können dann unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden.
In den Einzelfällen, in denen das Arbeiten mit breiten Einwilligungen als für das Erreichen des Forschungszwecks zwingend erforderlich erachtet wird, ist deshalb insbesondere mit den folgenden Korrektiven

zu arbeiten. Sie dienen der Transparenz, Vertrauensbildung und Datensicherheit, um die abstraktere Fassung des Forschungszwecks zu kompensieren:

A. Zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz

- Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet
- Ausarbeitung und Dokumentation im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung der Forschungszwecke nicht möglich ist
- Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden.

B. Zusätzliche Sicherungsmaßnahmen zur Vertrauensbildung

- Positives Votum eines Ethikgremiums vor der Nutzung für weitere Forschungszwecke
- Prüfung, ob das Arbeiten mit einem dynamic consent möglich ist bzw. Einräumung einer Widerspruchsmöglichkeit vor der Verwendung der Daten für neue Forschungsfragen.

C. Zusätzliche Garantiemaßnahmen zur Datensicherheit

Verstärkter Einsatz von Garantien im Hinblick auf die erhobenen Daten durch technisch-organisatorische Maßnahmen wie:

- Keine Datenweitergabe in Drittländer mit geringerem Datenschutzniveau
- Gesonderte Zusagen zur Datenminimierung, Verschlüsselung, Anonymisierung oder Pseudonymisierung
- Spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten.

Das Ergebnis der Prüfung einschließlich der zugrundeliegenden Beweggründe sowie die Sicherstellung der o. g. Sicherungsmaßnahmen

sind zu dokumentieren und den zur Prüfung der ethischen und datenschutzrechtlichen Vereinbarkeit des Forschungsvorhabens zuständigen Stellen zusammen mit dem Forschungskonzept vorzulegen.

5.13 Beschluss: Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen
Stand: 26. April 2019

Zukünftig sollen nach einem Referentenentwurf zur Änderung des Rundfunkbeitragsstaatsvertrags (RBStV) regelmäßig alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt zur Sicherstellung der Aktualität des dortigen Datenbestandes übermittelt werden. Gemäß Art. 1 Ziffer 7 dieses Entwurfs des 23. Rundfunkänderungsstaatsvertrages vom 5. Februar 2019 zählen zu den Meldedaten neben Namen und gegenwärtiger und letzter Anschrift insbesondere auch Geburtstag, Titel, Familienstand sowie die genaue Lage der Wohnung.
Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war seinerzeit auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010). Die DSK stellte ihre Bedenken nur deshalb teilweise zurück, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Mit der nun vorgesehenen Regelung wären die – bereits damals zweifelhaften – Zusicherungen des Gesetzgebers, dass es sich bei den anlasslosen vollständigen Meldedatenabgleichen aus den Jahren 2013 und 2018 um einmalige Vorgänge handeln würde, endgültig hinfällig.
Gegen die geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs bestehen weiterhin grundlegende verfassungsrechtliche und datenschutzrechtliche Bedenken.
Ein solcher Abgleich stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und gerät in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO).
Bei einem vollständigen Meldedatenabgleich werden in großem Umfang personenbezogene Daten von Betroffenen, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen Beiträge gezahlt werden oder weil sie von der Beitragspflicht befreit sind, an die Rundfunkanstalten übermittelt und von diesen verarbeitet. Zudem werden auch Daten von

all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die sich bereits bei der Landesrundfunkanstalt angemeldet haben und regelmäßig ihre Beiträge zahlen. Dabei betrifft der geplante Meldedatenabgleich mehr personenbezogene Daten, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, z. B. Doktorgrad und Familienstand (vgl. § 8 Abs. 4 RBStV). Es sollen also personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die nicht zur Beitragserhebung notwendig sind.
Die Meldedaten-Übermittlungsverordnungen der Länder bieten mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten bereits eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes des Beitragsservices auch bei Veränderungen der Meldesituation der Beitragsschuldnerinnen und Beitragsschuldner zu gewährleisten. Auch wenn die Meldebehörden in Einzelfällen eine Änderungsmitteilung unterlassen sollten, würde ein erneuter vollständiger Meldedatenabgleich in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Beitragsschuldner eingreifen, ohne dass dies durch andere Gesichtspunkte, etwa das Ziel der Gebührengerechtigkeit, gerechtfertigt wäre.
Die Landesrundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldedatenabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (vgl. Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019).
Die geplanten Regelungen berücksichtigen zudem die Maßstäbe der DS-GVO nicht ausreichend. Nationale Datenschutzvorschriften müssen aufgrund des Anwendungsvorrangs europäischer Verordnungen auf eine Öffnungsklausel der DS-GVO gestützt werden können. Art. 85 Abs. 2 DS-GVO ist nicht einschlägig, da die Datenverarbeitung zum Zweck des Einzugs des Rundfunkbeitrags nicht in dem Anwendungsbereich dieser Norm liegt. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e) DS-GVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Mitgliedstaatliche Regelungen für die Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, dürfen danach eingeführt werden, wenn diese die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich

in dem Rahmen halten, den die DS-GVO vorgibt. Hier bestehen erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.
Positiv hervorzuheben ist zwar, dass die bisherige Vermieterauskunft im Hinblick auf Mietwohnungen aus § 9 Abs. 1 Satz 2 und 3 RBStV gestrichen werden soll. Ebenso soll der Ankauf von Adressdaten von Privatpersonen ausdrücklich ausgeschlossen werden. Beide Datenverarbeitungen sind aus Sicht des Datenschutzes kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich eine weitaus umfassendere, datenschutzrechtlich ebenfalls sehr bedenkliche Möglichkeit der Datenerhebung geschaffen werden soll, die das praktische Bedürfnis der Vermieterauskunft und des Ankaufs privater Adressen ohnehin entfallen lässt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen.

5.14 Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU
Stand: 13. Mai 2019

1. Die Verpflichtung zur Beteiligung der spezifischen Aufsichtsbehörden nach § 18 Abs. 1 Satz 4 BDSG ist nur dann eröffnet, wenn es sich um Angelegenheiten der Europäischen Union handelt.
2. Liegen die Voraussetzung von Nr. 1 vor, ist eine Betroffenheit in folgenden Konstellationen gegeben:
a) eine spezifische Aufsichtsbehörde ist im Kooperationsverfahren nach Art. 60 DSGVO unmittelbar selbst federführende Behörde im Sinne von § 19 Abs. 1 BDSG (vgl. Art. 56 DSGVO);
b) eine spezifische Aufsichtsbehörde ist für die Bearbeitung einer Eingabe entsprechend § 19 Abs. 2 BDSG (vgl. Art. 4 Nr. 22 Buchst. c DSGVO) zuständig;
c) eine spezifische Aufsichtsbehörde ist in entsprechender Anwendung von § 40 Abs. 2 BDSG in der Rolle als betroffene Behörde (vgl. Art. 4 Nr. 22 Buchs. a DSDGVO) zuständig;
d) eine spezifische Aufsichtsbehörde ist in den Verfahren nach Art. 60 DSGVO in der Konstellation des Art. 4 Nr. 22 Buchst. b DSGVO betroffen, wenn sich die erheblichen Auswirkungen nur im Rahmen der ausschließlichen Zuständigkeiten der spezifischen Aufsichtsbehörde bewegen;
e) ein Verfahren der Amtshilfe nach Art. 61 DSGVO oder gemeinsame Maßnahmen spielen sich unmittelbar im Zuständigkeitsbereich einer spezifischen Aufsichtsbehörde ab.
3.
a) Im Kohärenzverfahren nach Art. 64 DSGVO, ggf. zusätzlich im Verfahren der verbindlichen Streitbeilegung nach Art. 65 DSGVO (bei unmittelbarer Zuständigkeit siehe oben 2);
und

b) bei der Erarbeitung von Stellungnahmen und der Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren i. S. v. Art. 70 DSGVO liegt nur dann eine Betroffenheit vor, wenn spezifische Fragen der Verarbeitung personenbezogener Daten durch die der Aufsicht der spezifischen Aufsichtsbehörden unterliegenden Stellen betroffen sind.

Erläuterung: Spezifische Betroffenheit bedeutet, dass gerade die spezifische Aufsichtsbehörde in einer Weise von der Angelegenheit betroffen sein muss, die über eine allgemeine Mitbetroffenheit hinausgeht. Ist sie lediglich in gleicher Weise betroffen wie die staatlichen Aufsichtsbehörden, liegt keine spezifische Betroffenheit vor und die Beteiligungspflicht wird nicht ausgelöst. Dabei kommt es nicht nur darauf an, dass beispielsweise Kirchen, Religionsgemeinschaften oder Medien-/Rundfunkveranstalter ausdrücklich Gegenstand einer Angelegenheit sind. Eine spezifische Betroffenheit ist vielmehr auch dann anzunehmen, wenn der Gegenstand einer Angelegenheit in besonderer Weise den Zuständigkeitsbereich der spezifischen Aufsichtsbehörden berührt.
4. Die Aufsichtsbehörden des Bundes und der Länder können für alle weiteren Fälle eine Beteiligung vorsehen.
5. Die Verpflichtungen zur Beteiligung nach § 18 Abs. 1 Satz 4 BDSG sind erfüllt, wenn die spezifischen Aufsichtsbehörden frühzeitig mit allen zweckdienlichen Informationen versorgt sind und ihnen frühzeitig Gelegenheit zur Stellungnahme gegeben wird. Die Betroffenheit einer spezifischen Aufsichtsbehörde wird von der Aufsichtsbehörde geprüft, die die Herstellung einer Positionsbestimmung in europäischen Angelegenheiten initiiert. Die Beteiligung der spezifischen Aufsichtsbehörden wird über die Zentrale Anlaufstelle sichergestellt. Die Aufsichtsbehörden des Bundes und der Länder berücksichtigen die Stellungnahmen der spezifischen Aufsichtsbehörden. Eine abweichende Stellungnahme ändert aber weder etwas an einem sonst unter den Aufsichtsbehörden von Bund und Ländern bestehenden Einvernehmen noch hat dies Auswirkungen auf Abstimmungen nach § 18 Abs. 2 BDSG.
6. Bei § 18 Abs. 1 Satz 4 BDSG handelt es sich um eine Verfahrensregelung, deren Nichteinhaltung keine rechtlichen Folgen für das Verfahren hat.
7. Die spezifischen Aufsichtsbehörden werden durch die Aufsichtsbehörden des Bundes und der Länder regelmäßig über die Entwicklungen auf europäischer Ebene informiert.
8. Gemeinsam mit dem BfDI lädt der Vorsitz der Datenschutzkonferenz Vertreter der spezifischen Aufsichtsbehörden zweimal jährlich zu einem Informations- und Erfahrungsaustausch ein.
9. Religions- und Weltanschauungsgemeinschaften können nach Artikel 91 Absatz 2 DSGVO nur dann eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, einrichten, wenn sie bereits zum

Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Art. 91 Abs. 1 DSGVO angewendet haben. Diese Datenschutzregelungen müssen mit der DSGVO in Einklang gebracht werden.
10. Weitere Erläuterungen ergeben sich aus den Arbeitsergebnissen der 9. Sitzung des AK Grundsatz, die die DSK am 29. Januar 2019 zustimmend zur Kenntnis genommen hat.

5.15 Asset Deal – Katalog von Fallgruppen

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[7]
Stand: 24. Mai 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich auf einen Katalog von Fallgruppen verständigt, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f i. V. m. Abs. 4 DS-GVO bei einem Asset Deal zu berücksichtigen sind. Die Fallgruppen lauten:

1. **Kundendaten bei laufenden Verträgen**
   Hier bedarf der Vertragsübergang zivilrechtlich einer Genehmigung der Kundin oder des Kunden (§ 415 BGB / Schuldübernahme). In dieser zivilrechtlichen Genehmigung wird als Minus auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten gesehen. Damit sind die Gegeninteressen der Kundin oder des Kunden gewahrt.
2. **Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als 3 Jahre**[8]
   Daten von Bestandskundinnen und -kunden, bei denen die letzte aktive Vertragsbeziehung mehr als 3 Jahre zurückliegt, unterliegen bei einer erwerbenden Stelle einer Einschränkung der Verarbeitung. Diese Daten dürfen zwar übermittelt, aber eben nur wegen gesetzlicher Aufbewahrungsfristen genutzt werden.
   Denkbare Alternative ist, dass entsprechende Kundendaten nicht übertragen werden, sondern beim Alt-Unternehmen verbleiben. Ist ein Insolvenzverwalter eingeschaltet, bemüht dieser sich um einen aus der Masse zu finanzierenden Dienstleister, der die Alt-Daten für einen bestimmten Zeitraum aufbewahrt.

[7] Unter Ablehnung der Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie des Sächsischen Datenschutzbeauftragten.
[8] Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als 3 Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

3. **Daten von Kundinnen und Kunden bei fortgeschrittener Vertragsanbahnung; Bestandskundinnen und -kunden ohne laufende Verträge und letzter Vertragsbeziehung jünger als 3 Jahre**[9]
   Daten solcher Kundinnen und Kunden werden nach Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO im Wege der Widerspruchslösung (Opt-out-Modell) mit einer ausreichend bemessenen Widerspruchsfrist (z. B. 6 Wochen) übermittelt. Diese Vorgehensweise ist für die Unternehmen aufwandsschonend und berücksichtigt durch die großzügige Widerspruchsfrist auch die Interessen der Kundinnen und Kunden. Viele Kundinnen und Kunden sind bei einer Aufforderung zu einer ausdrücklichen Einwilligung eher überrascht. Auch sollte darauf geachtet werden, den Widerspruch einfach auszugestalten – z. B. im Online-Verfahren durch Klick auf ein Kästchen.
   Die Bankdaten (IBAN) sind jedoch vom Übergang per Widerspruchslösung ausgenommen und nur nach ausdrücklicher Einwilligung des Kunden zu übermitteln. Darunter fällt nicht das Zahlungsverhalten.
4. **Kundendaten im Falle offener Forderungen**
   Die Übertragung offener Forderungen gegen Kundinnen und Kunden richtet sich zivilrechtlich nach den §§ 398 ff. BGB (Forderungsabtretung). In diesem Zusammenhang stehende Daten darf der Zedent (Alt-Gläubiger/Alt-Unternehmen) an den Zessionar (Neu-Gläubiger/Neu-Unternehmen) – gestützt auf Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO – (früher § 28 Abs. 1 Satz 1 Nr. 2 oder Abs. 2 Nr. 2 lit. a BDSG a. F.) – übermitteln. Überwiegende Gegeninteressen bestehen allerdings dann, wenn die Abtretung durch Vereinbarung ausgeschlossen ist (§ 399 2. Alt. BGB, § 354a HGB).
5. **Kundendaten besonderer Kategorie nach Art. 9 Abs. 1 DS-GVO**
   Solche Daten können nur im Wege der informierten Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DS-GVO übergeleitet werden.

[9] Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als 3 Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

5.16 Spezifische Aufsichtsbehörden

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder zu spezifischen Aufsichtsbehörden
Stand: 12. August 2019

Nach der Sonderregelung des Artikel 91 Absatz 1 der Europäischen Datenschutz-Grundverordnung (DSGVO) dürfen Kirchen, religiöse Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regelungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anwenden, diese weiter anwenden, sofern sie mit den Vorschriften der DSGVO in Einklang gebracht werden.
Grundsätzlich unterliegen auch die Kirchen, religiösen Gemeinschaften oder Vereinigungen, die bereits zum Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Artikel 91 Absatz 1 DSGVO angewendet haben, nach Artikel 91 Absatz 2 DSGVO der Aufsicht durch eine unabhängige Aufsichtsbehörde. Artikel 91 Absatz 2 DSGVO erlaubt ihnen jedoch, eine unabhängige Aufsichtsbehörde spezifischer Art einzurichten.
Für Religionsgemeinschaften, die erst nach dem Inkrafttreten der DSGVO umfassende Datenschutzvorschriften erlassen (haben), ist der sachliche Anwendungsbereich der DSGVO uneingeschränkt eröffnet und es gilt die allgemeine Datenschutzaufsicht.
Bei Artikel 91 handelt es sich um eine Bestandsschutzregelung für die Datenschutzvorschriften derjenigen Kirchen und religiösen Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO bereits ein umfassendes, in sich abgeschlossenes Datenschutzrecht etabliert hatten. Solche Religionsgemeinschaften sollen nicht gezwungen sein, ihr unter dem alten Recht bereits etabliertes Recht abschaffen zu müssen.
Die bestehenden Datenschutzregelungen müssen allerdings mit der DSGVO in Einklang gebracht worden sein. Dadurch soll trotz der Privilegierung dieser Regelungen ein einheitliches Niveau staatlichen und kirchlichen Datenschutzrechts erreicht werden.
Die „spezifischen“ Aufsichtsbehörden müssen darüber hinaus die in Kapitel VI der DSGVO für die unabhängigen Aufsichtsbehörden nie-

dergelegten Voraussetzungen erfüllen. Das betrifft u. a. die Unabhängigkeit, Artikel 52 DSGVO, und die in Artikel 58 DSGVO geregelten Befugnisse.
Die Datenschutzaufsichtsbehörden des Bundes und der Länder sind gemäß § 18 Absatz 1 Satz 4 Bundesdatenschutzgesetz (BDSG) verpflichtet, diese spezifischen Aufsichtsbehörden bei der Zusammenarbeit in europäischen Angelegenheiten zu beteiligen, soweit sie betroffen sind.
Durch Anpassung des jeweils bereits vor dem 25. Mai 2016 bestehenden Gesetzes über den Kirchlichen Datenschutz sowie des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland an die DSGVO unterfallen zumindest die römisch-katholische Kirche bzw. die Adressaten des EKD-Datenschutzgesetzes grundsätzlich der durch Artikel 91 DSGVO ermöglichten Privilegierung.

5.17 Datenschutzrechtliche Verantwortlichkeit innerhalb der Telematik-Infrastruktur

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 12. September 2019

Die Datenschutzkonferenz vertritt zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nach § 291a Abs. 7 SGB V folgende Auffassung:
Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) ist

a) datenschutzrechtlich alleinverantwortlich für die zentrale Zone der TI („TI-Plattform Zone zentral“) sowie
b) im Sinne des Artikel 26 DSGVO datenschutzrechtlich mitverantwortlich für die dezentrale Zone der TI („TI-Plattform Zone dezentral“). Der Umfang der Verantwortung der gematik für die dezentrale Zone der Telematik-Infrastruktur bedarf einer gesetzlichen Regelung. Die gematik ist verantwortlich für die Verarbeitung, insbesondere soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist.

5.18 Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 12. September 2019

Auf Basis des Urteils des EuGH vom 13. Juni 2019 (Az. C – 193/18) zur Auslegung des Begriffs des „Telekommunikationsdienstes“ gelten für die Zuständigkeitsverteilung zwischen dem BfDI und den Aufsichtsbehörden der Länder vorbehaltlich einer Änderung der gesetzlichen Zuständigkeitsregelungen folgende Grundsätze:

1. Webmaildienste sind keine Telekommunikationsdienste i. S. d. Telekommunikationsgesetzes (TKG) in der derzeit geltenden Fassung. Dies gilt für reine Webmaildienste und für E-Maildienste, die zusammen mit einem Internetzugang angeboten werden, wenn die E-Mails (zumindest auch) über einen Webmailer abgerufen werden können. Daraus folgt, dass für die Datenschutzaufsicht mangels anderer besonderer Zuständigkeitsvorschriften allein die jeweiligen Landesdatenschutzaufsichtsbehörden zuständig sind. Die bisher beim Bundesbeauftragten für den Datenschutz (BfDI) geführten Verfahren werden an die jeweils zuständigen Landesaufsichtsbehörden zur Bearbeitung zuständigkeitshalber abgegeben.

2. Messenger-Dienste, die in einem geschlossenen System operieren, d. h. bei denen die Nutzer/innen nur unter sich und nicht mit Nutzer/innen anderer Dienste kommunizieren können, können auch nach der genannten Entscheidung des EuGH als Telekommunikationsdienste i. S. d. TKG angesehen werden mit der Folge, dass für diese Dienste weiterhin der BfDI aufsichtsrechtlich zuständig ist (§ 115 Abs. 4 TKG).

5.19 Verhaltensbasierte Werbung

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 25. September 2019

Am 04.06.2019 legte das Netzwerk Datenschutzexpertise bei einigen deutschen Datenschutzaufsichtsbehörden eine Beschwerde wegen der Datenverarbeitung im Rahmen personalisierter Online-Werbung ein. Die Unterzeichner der Beschwerde sind allesamt Vorsitzende von Menschenrechts- und Digitalrechtsorganisationen und bezeichnen sich ausdrücklich als Beschwerdeführer.
In der Beschwerde wird die Datenverarbeitung durch Google sowie weitere Anbieter, die Mitglieder des IAB Europe sind, gerügt.
Die Beschwerde umfasst eine detaillierte Beschreibung der Datenverarbeitung von Werbenetzwerken und weist auf mögliche Verstöße gegen die DS-GVO hin.
Die Beschwerde richtet sich allgemein gegen die Datenverarbeitung von Werbenetzwerken und umfasst nicht nur die Verarbeitung durch Google. Weitere Anbieter bzw. Akteure werden jedoch nicht ausdrücklich genannt, sodass sich die Beschwerde zunächst nur gegen Google richtet.
Vor diesem Hintergrund fasst die Datenschutzkonferenz den folgenden Beschluss:

I. Die Beschwerde erfüllt die Anforderungen gem. Art. 77 DSGVO, da sie

   1. von natürlichen Personen als betroffenen Personen eingelegt wurden (die 4 Unterzeichner);
   2. sich gegen einen konkreten Verantwortlichen richtet (Google) und
   3. die betroffenen Personen beschwerdebefugt sind, da sie umfassend erläutern, dass die Datenverarbeitung bei der personalisierten Online-Werbung gegen die DS-GVO verstößt und sie dadurch in ihren Rechten verletzt werden.

II. Beschwerdegegner ist zunächst nur Google. Soweit sich die Beschwerde gegen dieses Unternehmen richtet, ist sie zunächst an den Hamburgischen Beauftragten weiterzuleiten.

III. Das IAB Europe ist kein Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO, da es sich beim IAB Europe lediglich um einen Interessenverband von Unternehmen aus dem Bereich Programmatic Advertising handelt.

IV. Sofern eine Aufsichtsbehörde der Auffassung ist, die Beschwerde sei dahingehend auszulegen, dass sich die Beschwerde gegen die jeweiligen Mitgliedsunternehmen des IAB Europe richtet, so ist mit der Beschwerde entsprechend Ziff. III. zu verfahren.

5.20 Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO

November 2019

Inhalt

Einleitender Überblick 4
Schwerpunktthema Nr. 1 – Alltagserleichterung & Praxistauglichkeit 7
I. Informationspflichten 7
1. Problemaufriss 7
2. Bewertung 7
3. Konkreter Änderungsvorschlag 8
II. Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO 9
III. Pflicht zur Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO 9
1. Problemaufriss 9
2. Bewertung 10
3. Konkreter Änderungsvorschlag 10
Schwerpunktthema Nr. 2 – Datenpannenmeldungen 11
I. Art. 33 Abs. 1 DS-GVO 11
1. Problemaufriss 11
2. Bewertung 11
3. Änderungsvorschlag 11
Schwerpunktthema Nr. 3 – Zweckbindung 13
1. Problemaufriss 13
2. Bewertung 13
3. Änderungsvorschläge 14
Schwerpunktthema Nr. 4 – data protection by design 15
1. Problemaufriss 15
2. Bewertung 16
3. Änderungsvorschläge 16
Schwerpunktthema Nr. 5 – Befugnisse der Aufsichtsbehörden und Sanktionspraxis 18
I. Befugnisse 18
1. Problemaufriss 18
2. Bewertung 18

3. Änderungsvorschläge 18
II. Art. 83 Abs. 5 lit. e DS-GVO – Sanktionen, Tatbestand für Verstöße gegen Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 1 lit. a DS-GVO 19
1. Problemaufriss 19
2. Bewertung 19
3. Änderungsvorschlag 19
Schwerpunktthema Nr. 6 – Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz 21
I. Art. 46 Abs. 4 i. V. m. Art. 64 Abs. 2 DS-GVO 21
1. Problemaufriss 21
2. Bewertung 21
3. Änderungsvorschlag 21
II. Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII 21 1. Problemaufriss 21
2. Bewertung 21
3. Änderungsvorschlag 22
III. Art. 64 Abs. 7 DS-GVO 22
1. Problemaufriss 22
2. Bewertung 22
3. Änderungsvorschlag 22
Schwerpunktthema Nr. 7 – Direktwerbung 23
1. Problemaufriss 23
2. Bewertung 23
3. Änderungsvorschlag 23
Schwerpunktthema Nr. 8 – Profiling 24
1. Problemaufriss 24
2. Bewertung 24
Schwerpunktthema Nr. 9 – Akkreditierung 25
1. Problemaufriss 25
2. Bewertung 25
3. Änderungsvorschläge 25
Liste weiterer Änderungsvorschläge 26

Einleitender Überblick

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hat den folgenden Bericht über die Erfahrungen bei der Anwendung der DS-GVO

erarbeitet und auf der 98. DSK am 06. November 2019 verabschiedet. Die DSK möchte damit die Erfahrungen der in ihr vertretenen deutschen Aufsichtsbehörden aus der praktischen Anwendung seit Geltungsbeginn der DS-GVO in den Evaluierungsprozess nach Art. 97 DS-GVO einbringen und daran anknüpfend in einigen Punkten auch Vorschläge für Verbesserungen unterbreiten, um einen optimalen Vollzug der DS-GVO zu gewährleisten.
Nach einem Jahr der Geltung der DS-GVO zieht die Europäische Kommission im Juli 2019 zu Recht eine positive Bilanz. Die DS-GVO habe die EU-Bürger zunehmend auf die Datenschutzbestimmungen und ihre Rechte aufmerksam gemacht, die Unternehmen passen ihre Praktiken an, sie erhöhen die Sicherheit ihrer Daten und entwickeln den Datenschutz als Wettbewerbsvorteil. Die Verordnung habe den nationalen Datenschutzbehörden mehr Befugnisse zur Durchsetzung der Vorschriften gegeben. Im ersten Jahr haben die nationalen Datenschutzbehörden diese neuen Befugnisse bei Bedarf wirksam genutzt, sie arbeiten im Rahmen des Kooperationsmechanismus enger zusammen.
Die DSK teilt die Auffassung, dass sich die DS-GVO mit ihrem Regelungskonzept und ihren Zielen im Wesentlichen bewährt. Die Ziele des verbesserten Grundrechtsschutzes und der Schaffung eines einheitlichen digitalen Binnenmarktes erscheinen durch die DS-GVO vorangebracht und auch tatsächlich erreichbar.
Als ein zentraler Aspekt der gesellschaftlichen Wahrnehmung und als Motor zur Entwicklung eines breitangelegten datenschutzrechtlichen Bewusstseins erwies sich, dass bei Verstößen gegen Datenschutznormen erstmals empfindliche Geldbußen drohen. Behörden und Betriebe stellen sich den Anforderungen. Sie agieren aber teilweise unsicher, Umsetzungsdefizite sind zu beobachten. Die Vorgaben an die Verantwortlichen sind vielfältig (die DS-GVO selbst, die Erwägungsgründe, Guidelines), sodass ein umfassendes Datenschutzmanagement des Verantwortlichen geboten ist.
Dazu bedarf es einer Interpretation der Vorgaben, die unzählige Datenschutzberater anbieten. Der Bedarf, Orientierung durch die Aufsichtsbehörden zu erhalten ist noch immer sehr hoch. Dieser erhöhten Nachfrage begegneten die Aufsichtsbehörden mit einer intensiven Beratungstätigkeit, deren Kern darin besteht aus einer gestiegenen Anzahl von Rechts- und Informationsquellen einen roten Faden zu wirken, der es erlaubt, den Verantwortlichen pragmatische Handlungs-

empfehlungen zu geben. Die so gestiegene Akzeptanz des Datenschutzrechts und der Arbeit der Aufsichtsbehörden muss nunmehr erhalten und ausgebaut werden.
In dieser Hinsicht sind die durch die enorm gestiegene Anzahl von Beschwerden, durch aufwändige grenzüberschreitende Zusammenarbeit (IMI) und intensivierte Beratung gestiegenen Anforderungen an die Aufsichtsbehörden teilweise nicht mit auskömmlicher Aufstockung an Personal und Sachmitteln begleitet worden. Gemäß Art. 52 Abs. 4 DS-GVO hat jeder Mitgliedstaat sicherzustellen, dass seine Aufsichtsbehörde mit den Ressourcen, „die sie benötigt“, ausgestattet wird.
Dies hat u. a. zur Folge, dass von einigen Aufsichtsbehörden anlasslose Kontrollen nicht im erforderlichen Maße durchgeführt werden können, so dass Verantwortliche ein Kontrolldefizit erkennen und in ihren Bemühungen zur Schaffung datenschutzkonformer Zustände nachlassen.
Neben den gesetzlich für die Evaluierung der DS-GVO durch die Kommission festgelegten Themen des Art. 97 Abs. 2 DS-GVO wurde der Fokus des vorliegenden Berichts auf etwaigen Änderungsbedarf aufgrund der Anwendungs-Erfahrungen im ersten Geltungsjahr der DS-GVO gelegt. Dies sowohl bezogen auf bestehende Vorschriften als auch auf die möglicherweise notwendige Schaffung weiterer Regelungen. Auch die Erwägungsgründe wurden in die Überlegungen miteinbezogen.
Die Frage der Befassung mit etwaigen Problemen bei der Umsetzung der DS-GVO in Bundes- und Landesrecht wurde nicht in den Bericht miteinbezogen. Soweit einzelne nationale Umsetzungsnormen problematisch oder kritikwürdig erscheinen, kann sich hieraus allerdings auch ein Änderungsbedarf an Öffnungsklauseln der DS-GVO ergeben.
Grundsätzlich nicht berücksichtigt oder auf essentielle Punkte reduziert wurden außerdem Klarstellungs-, Auslegungs-, Definitions- und Übersetzungsprobleme. Auch strittige Punkte, welche sich bereits im Gesetzgebungsverfahren abgezeichnet und bis heute als in der Anwendung problematisch erwiesen haben, wurden weitestgehend ausgeklammert.
Im Ergebnis haben sich im Zuge der Anwendung der DS-GVO bisher folgende Schwerpunktthemen herausgestellt:

1. Alltagserleichterung & Praxistauglichkeit
2. Datenpannenmeldungen
3. Zweckbindung
4. data protection by design
5. Befugnisse der Aufsichtsbehörden und Sanktionspraxis
6. Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz
7. Direktwerbung
8. Profiling
9. Akkreditierung

Bei den **Informations- und Transparenzpflichten** nach Art. 13 und 14 DS-GVO haben sich in der Praxis Umsetzungsprobleme gezeigt, z. B. bei telefonischer Datenerhebung. Hier geht es insbesondere um die Frage, ob zunächst eine allgemeinere Information an zentraler Stelle ausreicht und konkrete Informationen nur auf Verlangen nachgereicht werden können. Auch Umfang und Inhalt der Informationspflichten könnten möglicherweise praktikabler und bürgerfreundlicher definiert werden. In der Praxis stellt sich teilweise die Frage nach der **Alltagstauglichkeit** der Regelungen der DS-GVO. Möglichkeiten zur erleichterten Anwendung der Informationspflichten, die Pflicht zur Meldung von Datenschutzbeauftragten an die Aufsichtsbehörden sowie das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO wurden in den Fokus genommen.
Eine allgemein umgreifende Sorge vor den Sanktionsmöglichkeiten der DS-GVO führt nach der Erfahrung der Aufsichtsbehörden dazu, dass viele **Datenpannen** gemeldet werden, welche tatsächlich gar keine Datenpannen sind oder deren Risiken schon längst beseitigt wurden. Daher waren exorbitante Steigerungsraten bei den Meldungen von Datenpannen zu verzeichnen.
Im Bereich der **Zweckbindung** haben sich in der Praxis vor allem Fragen im Hinblick auf die Rechtsgrundlage und die Voraussetzungen der Weiterverwendung der personenbezogenen Daten bei der Zweckänderung ergeben.
Data protection by design findet in der Praxis kaum Resonanz, da der Anwendungsbereich der DS-GVO Hersteller gerade nicht erfasst. Die DS-GVO stellt mit data protection by design / by default aber Grundsätze auf, die sich in der Sache an Hersteller richten, nimmt diesen aber nicht als Verantwortlichen in die Pflicht. Daher wird die Frage aufgeworfen, ob auch Hersteller, Lieferanten, Importeure und

Verkäufer in die Pflicht genommen werden sollten, so wie es im Produkthaftungsrecht bereits der Fall ist.
Im Schwerpunktthema **„Befugnisse der Aufsichtsbehörden und Sanktionspraxis“** haben sich insbesondere Fragen nach dem Begriff des „Verarbeitungsvorgangs“ aus Art. 58 Abs. 2 lit. b DS-GVO sowie der Zusammenarbeit und des Auskunftsrechts der Aufsichtsbehörden im Bußgeldverfahren als besonders dringlich erwiesen. In einem weiteren in Art. 97 Abs. 2 lit. b DS-GVO aufgeführten Schwerpunkt werden die Erfahrungen der Aufsichtsbehörden mit den Themen **„Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz“** dargestellt.
Bei der **Direktwerbung** stellt sich in unterschiedlichen Konstellationen die Frage der Zulässigkeit, welche durch die Schaffung einer spezifischen Rechtsgrundlage gelöst werden könnte.
Als eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit wird das **Profiling** angesehen. Trotz vorhandener Begriffsdefinition wird der Prozess der Profilbildung als solcher von den meisten Normen der DS-GVO, etwa zur automatisierten Entscheidungsfindung, nicht erfasst, sodass eine Beurteilung meist nur nach den allgemeinen Tatbeständen des Art. 6 DS-GVO erfolgt. Die DSK fordert eine Verschärfung des geltenden Rechtsrahmens, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen.
Beim Schwerpunkt **Akkreditierung** könnte durch eine Klarstellung in der DS-GVO eine erhebliche nationale Zuständigkeitsfrage geklärt und die Aufsicht durch die deutschen Datenschutzaufsichtsbehörden sichergestellt werden.
In einer kurzen Liste weiterer Änderungsvorschläge sind konkrete Textänderungen samt Kurzbegründung aufgeführt, welche keinem Schwerpunktthema zuzuordnen sind, aber weitere Erleichterungen in der Anwendung der DS-GVO ermöglichen würden.
Zum aktuell vorherrschenden Thema in der wissenschaftlichen Auseinandersetzung – der Frage des Datenschutzes im Bereich der **Künstlichen Intelligenz** und automatisierten Entscheidungsverfahren – übersendet die DSK außerdem ihre „Hambacher Erklärung zur Künstlichen Intelligenz - Sieben datenschutzrechtliche Anforderungen“ vom 3. April 2019 im Anhang zur Kenntnis. Wenngleich die enthaltenen Forderungen sich auf zukünftige Fall- und Normkonstellationen beziehen, halten die deutschen Datenschutzaufsichtsbehörden die Be-

achtung dieser Grundsätze in den zukünftigen Evaluierungsprozessen für unerlässlich.

Schwerpunktthema Nr. 1 – Alltagserleichterung & Praxistauglichkeit

Bei der Beratung, Fallbearbeitung sowie dem Austausch mit Verantwortlichen ist den deutschen Datenschutzaufsichtsbehörden häufig Unverständnis für die Regelungen beziehungsweise den Umfang der Informationspflichten, des Verzeichnisses der Verarbeitungstätigkeiten sowie der Notwendigkeit von Datenschutzfolgenabschätzungen entgegengeschlagen. Vor allem kleine und mittlere Unternehmen (KMU) sowie nicht-gewerbliche Vereine fühlen sich in Deutschland durch die Vorgaben der DS-GVO übermäßig belastet und fordern Ausnahmeregelungen.

I. Informationspflichten

1. Problemaufriss

Die in Art. 13 und 14 DS-GVO geregelten Informations- und Transparenzpflichten sind ein Kernstück der Datenschutz-Grundverordnung. Die deutschen Aufsichtsbehörden erachten das u. a. in Art. 12 Abs. 1 DS-GVO ausgedrückte Anliegen, die betroffene Person in verständlicher und angemessener Form über ihre Datenschutzrechte zu informieren, für eine der wesentlichen Neuerungen durch die DS-GVO.

Teilweise wurde an deutsche Aufsichtsbehörden die Befürchtung herangetragen, die Erfüllung der Informationspflichten sei für Verantwortliche, wie z. B. Vereine und KMU möglicherweise zu aufwändig. Jedoch können auch kleine Einrichtungen Datenverarbeitungen vornehmen, die tiefgreifende Auswirkungen auf die Betroffenen haben.

Einige Verantwortliche haben außerdem gegenüber deutschen Aufsichtsbehörden Probleme adressiert, die bei der Erfüllung der Informationspflichten in bestimmten Kontexten auftreten, wie z. B. bei telefonischer Terminabsprache oder telefonischem Vertragsschluss und der damit verbundenen Datenerhebung.

Als Lösungsansatz wird zum Teil die Einführung einer an Art. 30 Abs. 5 DS-GVO angelehnten Ausnahme für Vereine und KMU mit unter 250 Mitarbeitern vorgeschlagen. Ein weiterer, am Risiko für die Betroffenen orientierter Lösungsansatz ist eine Reduzierung der In-

formationspflicht in Fällen, in denen die Datenverarbeitung sich in einem sehr engen und für die Betroffenen erwartbaren Rahmen hält.

2. Bewertung

Die Aufsichtsbehörden befürworten grundsätzlich einzelne Praxis-Erleichterungen, warnen aber vor generellen Ausnahmen von Verantwortlichen-Pflichten.

Aus den Erfahrungen der Aufsichtsbehörden in der Beratung von Unternehmen, deren Datenverarbeitung hauptsächlich im Rahmen von Kundenbeziehungen stattfindet, ergibt sich für gewisse Fallgestaltungen ein Bedarf an Erleichterungen bei den Informationspflichten. In der Bewertung kann zwischen einer digitalen und einer nicht digitalen Umgebung unterschieden werden.

In einer digitalen Umgebung sind die Informationspflichten regelmäßig gut erfüllbar. Gemäß ErwG 58 Satz 2 DS-GVO können die Informationen grundsätzlich in elektronischer Form zum Zeitpunkt der Erhebung bereitgestellt werden. Sofern der Verantwortliche eine Webseite betreibt, kann von ihm erwartet werden, die erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ anzubieten.

In bestimmten nicht digitalen Sachverhalten führt jedoch das Erfordernis der Information zum Zeitpunkt der Erhebung gemäß Art. 13 DS-GVO zu praktischen Zweifelsfragen. Vor allem bei mündlichen oder telefonischen Kontakten im geschäftlichen Bereich ist es lebensfremd zu erwarten, dass der Verantwortliche, wenn er eine Bestellung aufnimmt, eine Visitenkarte entgegennimmt oder einen Termin notiert, umfassende Informationen gemäß Art. 13 Abs. 1 und 2 DS-GVO erteilt, also die Rechtsgrundlage benennt, über die zuständige Datenschutzaufsichtsbehörde oder über Auskunfts-, Beschwerde- und sonstige Betroffenenrechte und anderes mehr informiert. Eine solche Information würde auch häufig auf das Unverständnis der Betroffenen stoßen und von diesen als störend empfunden werden.

Art. 13 Abs. 4 DS-GVO schließt die Informationspflichten zwar praxisgerecht aus, wenn und soweit die betroffene Person bereits über die Informationen verfügt; gerade im Rahmen von Unternehmen-Kunden-Beziehungen sind dem beauftragenden Kunden viele der informationspflichtigen Daten bereits bekannt. Nicht als bekannt vorausgesetzt werden kann grundsätzlich aber beispielsweise die Rechtsgrundlage der Datenverarbeitung (vgl. Art. 13 Abs. 1 lit. c DS-GVO). Diese ist jedoch nicht bei jeder Auftragserteilung, Terminvereinbarung etc.

von Interesse. Betroffene klagten an dieser Stelle häufig über eine Informationsflut. Unter Berücksichtigung des risikobasierten Ansatzes bei der Beauftragung beispielsweise eines Handwerksbetriebs mit risikoarmer Datenverarbeitung würde es hier auch aus Sicht der Betroffenen genügen, wenn sie auf die Auffindbarkeit der Informationen hingewiesen werden.
In Einklang mit dem Working Paper der Art. 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01), sprechen sich die deutschen Aufsichtsbehörden grundsätzlich dafür aus, die in Art. 13 DS-GVO genannten Informationspflichten in einem gestuften Verfahren erfüllen zu können. In geeigneten Fällen können die notwendigen Informationen beispielsweise auch mit der Übersendung einer Auftragsbestätigung, durch Aushang im Ladengeschäft oder auf ähnliche Weise erteilt werden. Von generellen Ausnahmen sollte allerdings abgesehen werden, um dem Ziel der Vorschrift nicht zuwider zu laufen.

3. Konkreter Änderungsvorschlag
Einfügen eines neuen Absatzes in Art. 13 DS-GVO:

> Die Informationen nach den Absätzen 1 und 2 werden nur auf Verlangen der betroffenen Person mitgeteilt, soweit der Verantwortliche Datenverarbeitungen vornimmt, die der Betroffene nach den konkreten Umständen erwartet oder erwarten muss und
> 1. sowohl die Offenlegung von Daten gegenüber anderen Stellen als auch die Übermittlung in Drittländer ausgeschlossen sind,
> 2. keine Daten verarbeitet werden, die unter Art. 9 DS-GVO fallen,
> 3. die Daten nicht zu Zwecken der Direktwerbung verarbeitet werden und
> 4. weder Profiling noch automatisierte Entscheidungsfindungen stattfinden.
>
> Die betroffene Person ist auf diese Möglichkeit hinzuweisen.

Außerdem sollte eine Ausnahme von den Informationspflichten zum Zeitpunkt der Erhebung für die Fälle vorgesehen werden, in denen Daten auf der Grundlage von Art. 6 Abs. 1 lit. d DS-GVO verarbeitet werden.
Begründung: Mit diesem Vorschlag soll der risikobasierten Betrachtung bei den Alltagserleichterungen Ausdruck verliehen werden.

II. Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO

Das Auskunftsrecht nach Art. 15 DS-GVO ist eines der grundlegenden Betroffenenrechte. Ohne Informationen über die Verarbeitung ihrer personenbezogenen Daten können die betroffenen Personen ihre weiteren Rechte, wie z. B. das Recht auf Berichtigung oder Löschung oder das Recht zur Beschwerde bei einer Aufsichtsbehörde nicht effektiv wahrnehmen.
Allerdings ist die Weite des Auskunftsanspruchs umstritten, insbesondere in welchem Umfang Art. 15 Abs. 3 DS-GVO ein „Recht auf Kopie“ einräumt. Ein solches könnte den betroffenen Personen ermöglichen, vom Verantwortlichen die Herausgabe sämtlicher verarbeiteter personenbezogener Daten im Originalkontext zu verlangen. In der Praxis verlangen betroffene Personen zum Teil ohne nähere Konkretisierung Herausgabe aller beim Verantwortlichen vorhandenen Dokumente, die personenbezogene Daten enthalten. Dieser Anspruch kann z. B. auf die Kopie ganzer Verfahrensakten durch eine Behörde gerichtet sein oder auf die Herausgabe des gesamten geschäftlichen E-Mail-Verkehrs eines ehemaligen Mitarbeiters durch ein Unternehmen. Eine Klarstellung hinsichtlich des Umfangs des von Art. 15 Abs. 3 DS-GVO gewährten Rechts erscheint wünschenswert.

III. Pflicht zur Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

1. Problemaufriss

In Art. 37 Abs. 7 DS-GVO wird derzeit eine Pflicht konstatiert, der Aufsichtsbehörde Kontaktdaten von Datenschutzbeauftragten mitzuteilen. Die Verantwortlichen und Auftragsverarbeiter müssen gewährleisten, dass deren Meldung/en stets auf aktuellem Stand sind. Sie müssen diese nachhalten und ggf. gegenüber der zuständigen Aufsichtsbehörde korrigieren.
Durch die Pflicht, neben der Veröffentlichung der Kontaktdaten diese auch den Aufsichtsbehörden zu melden und beständig zu aktualisieren, entsteht bei den Verantwortlichen ein zusätzlicher Verwaltungsaufwand. Auf Seiten der Aufsichtsbehörden wird hierdurch eine nicht erforderliche Datenverarbeitung in Form einer Entgegennahme von Erst-, Änderungs- und Löschungsmeldungen ausgelöst. Teilweise wird Art. 37 Abs. 7 DS-GVO so interpretiert, dass die Aufsichtsbehörden ein Register der Datenschutzbeauftragten zu führen hätten

(inkl. der Verpflichtung, eine Vollständigkeit sicherzustellen und Unstimmigkeiten von Amts wegen zu bereinigen). Eine Vollständigkeit und Richtigkeit kann nur angestrebt, aber nie ganz erreicht werden. Im Hinblick auf die Tatsache, dass im nicht-öffentlichen Bereich ohne nähere Kenntnis der Organisation und des Geschäftsmodells des Verantwortlichen nicht über eine Benennungspflicht entschieden werden kann, sind dafür umfangreiche Datenerhebungen im Rahmen von Anhörungen erforderlich.

2. Bewertung

In der Praxis ist das Bereithalten von Kontaktdaten der oder des Datenschutzbeauftragten bei den Aufsichtsbehörden nicht erforderlich, da es eine Veröffentlichungspflicht gibt (Art. 37 Abs. 7 erster Satzteil DS-GVO). Bei Erstkontakten einer Aufsichtsbehörde mit Verantwortlichen könnten ggf. aktuelle Kontaktdaten der oder des Datenschutzbeauftragten mitgeteilt werden.
Zur Entlastung der Verantwortlichen bzw. Auftragsverarbeiter und der Datenschutzaufsichtsbehörden sollte diese Meldepflicht und die nicht erforderliche Datenverarbeitung, die zudem mangels Aktualität der Meldungen ungeeignet ist, entfallen.

3. Konkreter Änderungsvorschlag

In Art. 37 Abs. 7 DS-GVO sollte der letzte Halbsatz „und teilt diese Daten der Aufsichtsbehörde mit“ ersatzlos gestrichen werden.

Schwerpunktthema Nr. 2 – Datenpannenmeldungen

I. Art. 33 Abs. 1 DS-GVO

1. Problemaufriss

Nach Art. 33 Abs. 1 DS-GVO ist grundsätzlich jede Datenschutzverletzung der Aufsichtsbehörde zu melden. Eine Ausnahme besteht nur dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DS-GVO als Verletzung der Sicherheit legal definiert, die zu Vernichtung, Verlust, zur Veränderung oder unbefugten Offenbarung führt, und somit mit Art. 5 Abs. 1 lit. f) DS-GVO korrespondiert. Nach dem ErwG 85

DS-GVO kann die Verletzung des Schutzes einen physischen, materiellen oder immateriellen Schaden nach sich ziehen.
Da nach der vorherigen nationalen Rechtslage (§ 42a BDSG aF) eine Meldung nur bei bestimmten Datenarten erfolgen musste, hat sich die Zahl der Meldungen in der Bundesrepublik Deutschland deutlich erhöht. Für die Verantwortlichen besteht darüber hinaus die Schwierigkeit, einzuschätzen, in welchen Fällen kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Häufig dürfte dieses Risiko von Faktoren abhängen, die dem Verantwortlichen nicht bekannt sind. Darüber hinaus melden viele Verantwortliche vermeintliche Verstöße aus Furcht vor hohen Bußgeldern, ohne dass sie eine Risikoabwägung vorgenommen haben. Die sehr weite Fassung des Abs. 1 („voraussichtlich kein Risiko“) führt somit dazu, dass in sehr vielen Trivial- und Bagatellfällen Meldungen erfolgen, die eine hohe Belastung für die Aufsichtsbehörden darstellen und letztlich den Blick auf wirklich relevante Fälle verstellen.

2. Bewertung

Ein Risiko für die Rechte und Freiheiten natürlicher Personen kann in der Regel nicht vollkommen ausgeschlossen werden. Die Meldepflicht sollte daher auf Fälle beschränkt werden, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen.
Darüber hinaus sollte Art. 33 Abs. 1 DS-GVO auf Fälle ausgeweitet werden, bei denen nicht bekannt ist, ob eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat, diese aber zu vermuten ist. Häufig liegt eine Verletzung der Sicherheit von Daten vor, es ist aber nicht bekannt, ob dies zu einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO geführt hat.
Beispiel: Eine Dump (eine Kopie) einer umfangreichen Kundendatenbank war über Monate ungesichert über das Web zugänglich, Logfiles, über die ein Zugriff ausgeschlossen werden kann, liegen aber nur für wenige Tage vor. Eine Verletzung im Sinne von Art. 4 Nr. 12 DS-GVO kann (je nach Auslegung des Begriffs „Offenlegen“) hier nicht positiv festgestellt werde.
Hier sollte, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ist, eine Meldepflicht bestehen, sofern voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist.

3. Änderungsvorschlag

Art. 33 Abs. 1 Satz 1 und 2 DS-GVO neu, der bisherige Satz 2 wird zu Satz 3:

> Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich nicht nur zu geringen Risiken für die Rechte und Freiheiten natürlicher Personen führt, meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde. Darüber hinaus meldet der Verantwortliche einen Verstoß gegen die Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DS-GVO, die wahrscheinlich zur Verletzung des Schutzes personenbezogener Daten geführt hat oder führen wird, unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung der Sicherheit bekannt wurde, sofern im Fall der Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Schwerpunktthema Nr. 3 – Zweckbindung

1. Problemaufriss

Das Prinzip der Zweckbindung ist ein tragendes Prinzip des Datenschutzrechts. Es ist für die betroffenen Personen von praktisch sehr hoher Bedeutung, ob Daten, die sie einem Verantwortlichen zu bestimmten Zwecken preisgegeben haben, für andere Zwecke Verwendung finden dürfen. Die DS-GVO stellt daher besondere Voraussetzungen für die Weiterverarbeitung zu anderen Zwecken auf und sieht bei erlaubten zweckändernden Verarbeitungen eine Informationspflicht des Verantwortlichen vor.

Bei Anwendung des Art. 6 Abs. 4 DS-GVO gibt es Uneinigkeit darüber, ob für die zweckändernde Verarbeitung, die die Voraussetzungen des Art. 6 Abs. 4 DS-GVO an die Vereinbarkeit der Zwecke erfüllt, eine eigene Rechtsgrundlage erforderlich ist. Verantwortliche berufen sich z. B. bei der Weiterverwendung von Daten, die nach dem Gesetz, das ihnen die Datenverarbeitung erlaubt, streng zweckgebunden sind, darauf, dass nach ErwG 50 S. 2 DS-GVO für die zweckändernde Weiterverarbeitung keine eigene Rechtsgrundlage erforderlich sei, wenn der neue Zweck mit dem alten vereinbar ist. Demgegenüber haben jedoch betroffene Personen, die z. B. Daten gegenüber einem Verantwortlichen ohne rechtliche Verpflichtung preisgegeben haben,

ein großes Interesse daran, auch vor einer Weiterverwendung zu einem neuen Zweck erneut über die Preisgabe der Daten entscheiden zu können. Deutsche Aufsichtsbehörden haben in derartigen Konflikten unter Berufung auf Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 DS-GVO sowie auf ErwG 50 S. 8 DS- GVO gefordert, dass auch die zweckändernde Datenverarbeitung einer Rechtsgrundlage bedarf.
Abgesehen von dieser Frage hat sich in der Praxis die Privilegierung von Wissenschaft und Forschung in Art. 5 Abs. 1 lit. b i. V. m. Art. 6 Abs. 4 DS-GVO als zu weitgehend erwiesen.

2. Bewertung

Nach Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 1 DS-GVO muss jede Datenverarbeitung mindestens eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllen, um rechtmäßig zu sein. Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DS-GVO) und Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) sind zwei unterschiedliche, nebeneinander stehende Prinzipien der Datenverarbeitung. Die Vorschrift des Art. 6 Abs. 4 DS-GVO betrifft das Prinzip der Zweckbindung. Hätte im Rahmen dieser Vorschrift eine Ausnahme von dem Erfordernis einer Rechtsgrundlage gemacht werden sollen, so hätte dies angesichts der Bedeutung und Konsequenzen einer solchen Ausnahme ausdrücklich im Verordnungstext geregelt werden müssen.
Art. 6 Abs. 4 DS-GVO spricht nur von der Vereinbarkeit der Zwecke. Sein Satz 1 sagt aus, dass bei zweckändernden Verarbeitungen, die nicht auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a DS-GVO oder auf bestimmten Rechtsvorschriften der Union oder Mitgliedstaaten beruhen, die Vereinbarkeit der Zwecke geprüft werden muss. Nach dem Wortlaut bedeutet das nicht, dass bei diesen anderen zweckändernden Verarbeitungen die Prüfung der Vereinbarkeit des Zwecks die Rechtsgrundlage ersetzt, sondern, dass bei zweckändernden Verarbeitungen, die auf anderen Rechtsgrundlagen beruhen, eine Prüfung der Vereinbarkeit der Zwecke erfolgen muss. Die Regelung impliziert also gerade, dass alle zweckändernden Verarbeitungen auf einer Rechtsgrundlage beruhen müssen.
Insofern irritiert die Aussage in Satz 2 des ErwG 50 DS-GVO, in dem es heißt, es sei bei Vereinbarkeit der Zwecke „keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten“.
Auch wenn Satz 8 des gleichen ErwG konstatiert, dass in jedem Fall die in der Verordnung niedergelegten Grundsätze anzuwenden sind,

kann dies die Irritation nicht ganz beseitigen, da der Widerspruch zwischen dem nur auf die Rechtsgrundlage bezogenen Satz 2 und dem auf alle Grundsätze der DS-GVO bezogenen Satz 8 des ErwG 50 DS-GVO bestehen bleibt. Zum Teil wird der Verbleib des Satzes 2 in ErwG 50 nach den Trilogverhandlungen als Redaktionsversehen angesehen. In der Praxis führt er zu großen Schwierigkeiten bei der Durchsetzung der Rechtmäßigkeitsanforderungen an zweckändernde Datenverarbeitung und sollte daher gestrichen werden.

3. Änderungsvorschläge

ErwG 50 Satz 2 DS-GVO wird gestrichen.

Klarstellung in Art. 6 Abs. 4 DS-GVO: Weiterverarbeitungen auf Grundlage dieses Absatzes werden auf solche durch denselben Verantwortlichen beschränkt.

Schwerpunktthema Nr. 4 – data protection by design

1. Problemaufriss
Es sollten auch Hersteller, Lieferanten, Importeure, Verkäufer usw. in die Pflicht genommen werden, so wie dies im Produkthaftungsrecht (ProdHaftG bzw. RL 85/374/EWG) bereits der Fall ist.
Beim Begriff „Datenschutz durch Technikgestaltung“ (data protection by design), der in Art. 25 Abs. 1 DS-GVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus.
Verantwortliche entwickeln in der Regel nicht selbst Hard- und Software. Sie sind weitgehend auf Hardware und Standardbetriebssysteme und -anwendungssoftware angewiesen. Auf Anbieterseite bestehen oft Mono- oder Oligopole, sodass Produkte und Einsatzbedingungen von der Anbieterseite diktiert werden können.
Die DS-GVO stellt mit „data protection by design / data protection by default“ Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Die Forderung nach
„data protection by design / data protection by default“ läuft, wenn sie ausschließlich an die Verantwortlichen gerichtet wird, häufig ins Leere.
Die DS-GVO sollte daher auch die Hersteller von Software zur Einhaltung dieses datenschutzfördernden Designprinzips verpflichten. In

der Praxis trifft dies insb. auf Hersteller von komplexer Software wie z. B. Betriebssystemen, Datenbankmanagementsystemen, Standard-Office- Paketen oder sehr speziellen Fachanwendungen zu.

Hierzu zwei Beispiele:

1. Betriebssysteme

Verantwortliche, die Server, Desktop-Computer, Notebooks, Tablets, Smartphones oder ähnliche Geräte betreiben, müssen eines der wenigen am Markt erhältlichen Betriebssysteme, die auf der jeweiligen Hardware laufen, einsetzen. In der Regel sind diese schon vorinstalliert. Nach derzeitiger Rechtslage ist es die Pflicht dieser Verantwortlichen, etwaige datenschutzrechtlich relevante Schwachstellen, Fehlkonfigurationen, aus ihrer Sicht unerwünschte Funktionen etc. zu finden und abzustellen. Den Hersteller trifft keine Pflicht, seine Produkte ohne diese Fehler auszuliefern.

2. Haustür-Schließzylinder mit App

Es gibt Schließsysteme für Haustüren, die ohne physischen Schlüssel auskommen. Der Berechtigte identifiziert sich mit seinem Smartphone, auf dem eine passende App läuft. Zwischen der App und dem (in einem Drittland ohne angemessenes Datenschutz-Niveau befindlichen) Hersteller findet Datenverkehr statt.

a) Setzt ein Unternehmen derartige Systeme ein, ist es selbst Verantwortlicher und muss Datenverarbeitungen verantworten, die es nicht durchschauen kann. Der Hersteller ist nicht effektiv greifbar.
b) Setzt eine Privatperson im Rahmen privat-familiärer Tätigkeit derartige Systeme ein, ist ein Verantwortlicher im Sinne der DS-GVO schon nicht vorhanden. Die Pflichten der DS-GVO treffen niemanden, gehen also ins Leere. Würde man hier den Importeur, Händler o. ä. in die Verantwortung nehmen können, so wäre für „den Datenschutz“ viel gewonnen.

2. Bewertung

Die bisherige Rechtslage widerspricht dem Ansatz von „data protection by design“ bzw. „by default“.

Entgegen ErwG 78 S. 4 DS-GVO werden Hersteller in keiner Weise ermutigt, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzu-

stellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“.
Damit bestehen nicht nur erhebliche Lücken im Bereich des Schutzes personenbezogener Daten (und anderer Daten, vgl. Richtlinie (EU) 2016/943), sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral Mängel zu beseitigen, die zentral verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.
Die Rechtslage widerspricht so auch allgemeinem Recht. Nach dem über die RL 85/374/EWG harmonisierten Produkthaftungsrecht haften Hersteller für Schäden, die durch ihre Produkte entstehen. Neben Herstellern haften auch Importeure, Lieferanten, etc. Es gilt, diese bereits harmonisierte Rechtslage in den Bereich des Schutzes personenbezogener Daten zu übertragen.
Daher sollte Ziel sein, auch für datenschutzrechtlich relevante Produkte stärker auch die Hersteller in die Verantwortung zu nehmen.

3. Änderungsvorschläge

Durch die folgenden Änderungsvorschläge (unterstrichen dargestellt) würde die DS-GVO Pflichten für Hersteller usw. aufstellen, deren Durchsetzung aber dem Verbraucherschutz- und ggf. auch dem Wettbewerbsrecht überlassen.

Art. 4 - Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck …
27. „Hersteller“ den Hersteller im Sinne von Art. 3 der Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte. Nr. 16 Buchstabe a gilt entsprechend. Soweit er über Zwecke und Mittel der Datenverarbeitung entscheidet, ist der Hersteller auch Verantwortlicher im Sinne der Nr. 7.
KAPITEL IV - Verantwortlicher und Auftragsverarbeiter, Hersteller Abschnitt 1 - Allgemeine Pflichten
Art. 24 - Verantwortung des für die Verarbeitung Verantwortlichen und des Herstellers
(4) Der Hersteller entwickelt und gestaltet seine Produkte, Dienste und Anwendungen unter Berücksichtigung des Rechts auf Datenschutz und des Standes der Technik so, dass er sicherstellt, dass

Verantwortliche und Auftragsverarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen, ohne unzumutbare Änderungen an diesen Produkten, Diensten und Anwendungen vornehmen zu müssen. Er unterstützt sie bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30), bei der Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33) und bei der Benachrichtigung betroffener Personen (Art. 34), indem er ihnen auf Anfrage alle dazu notwendigen Informationen bereitstellt.

Art. 79 - Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche, Auftragsverarbeiter oder Hersteller
(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.
(2) Für Klagen gegen einen Verantwortlichen, gegen einen Auftragsverarbeiter oder gegen einen Hersteller sind die Gerichte des Mitgliedstaats zuständig, in dem der Hersteller, Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen, dem Auftragsverarbeiter oder dem Hersteller um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Art. 82 - Haftung und Recht auf Schadenersatz
(7) Beruht der Schaden ganz oder teilweise auf Handlungen oder Versäumnissen des Herstellers, so haftet dieser gegenüber der betroffenen Person neben dem Verantwortlichen oder Auftragsverarbeiter. Er haftet auch gegenüber dem Verantwortlichen und dem Auftragsverarbeiter.

Schwerpunktthema Nr. 5 – Befugnisse der Aufsichtsbehörden und Sanktionspraxis

I. Befugnisse

1. Problemaufriss

Die Worte „mit Verarbeitungsvorgängen“ in Art. 58 Abs. 2 lit. b DS-GVO führen zu Problemen bei der Anwendung der Vorschrift. Es gibt in der DS-GVO verschiedene Pflichten, die von einer konkreten Verarbeitung unabhängig sind, wie z. B. die Bestellung eines Datenschutzbeauftragten (Art. 37 DS- GVO) oder Vertreters (Art. 27 DS-GVO) oder die Pflicht zur Führung eines Verarbeitungsverzeichnisses (Art. 30 DS-GVO). Es ist deshalb für die Aufsichtsbehörden fraglich, auf welcher Rechtsgrundlage sie bei derartigen Verstößen eine Verwarnung aussprechen können.

2. Bewertung

Die Grundsätze, denen eine Verarbeitung entsprechen muss, sind in Art. 5 DS-GVO niedergelegt und in weiteren Vorschriften der DS-GVO genauer aufgeführt. Es gibt in der DS-GVO Pflichten, die von diesen Verarbeitungsgrundsätzen unabhängig sind. Zumindest für die Bestellung eines Datenschutzbeauftragten oder Vertreters oder für die Pflicht zur Führung eines Verarbeitungsverzeichnisses ist nicht ersichtlich, dass sie einen der in Art. 5 DS-GVO niedergelegten Grundsätze der Verarbeitung ausfüllen. Daher wird durch die Verletzung der genannten Pflichten die einzelne Verarbeitung nicht unzulässig. Es besteht aber ein praktischer Bedarf, auch bei derartigen Verstößen eine Verwarnung aussprechen zu können. Zur Vermeidung von Wertungswidersprüchen sollte diese Möglichkeit bei allen Verstößen gegen die Verordnung bestehen.
Zum Vergleich: Auch die Sanktionen in Art. 83 DS-GVO knüpfen nicht an Verarbeitungsvorgänge, sondern lediglich an „Verstöße gegen diese Verordnung“ (Abs. 1) bzw. „Verstöße gegen die folgenden Bestimmungen“ (Abs. 4, 5) an.

3. Änderungsvorschläge

Keine Beschränkung der Befugnisse nach Art. 58 Abs. 2 DS-GVO auf Verarbeitungsvorgänge.

Art. 58

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen, er voraussichtlich gegen diese Verordnung verstoßen wird,
b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, Maßnahmen oder die Erfüllung von Pflichten gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

II. Art. 83 Abs. 5 lit. e DS-GVO – Sanktionen, Tatbestand für Verstöße gegen Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 1 lit. a DS-GVO

1. Problemaufriss

Gemäß Art. 58 Abs. 1 lit. a DS-GVO kann der Verantwortliche / Auftragsverarbeiter von der Aufsichtsbehörde angewiesen werden, „alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind." Dieser behördliche Auskunftsanspruch verpflichtet den Adressaten, auf Anforderung der Behörde zuzuarbeiten.
Nach Art. 58 Abs. 1 lit. e DS-GVO hat die Aufsichtsbehörde darüber hinaus die Befugnis, „Zugang zu allen personenbezogenen Daten und Informationen zu erhalten, die zur Erfüllung ihrer Aufgabe notwendig sind." Das Zugangsrecht erlaubt der Aufsichtsbehörde, über die bereitgestellten Informationen hinaus in interne Unterlagen, Datenbanken und Verfahren Einsicht zu nehmen (z. B. Ehmann/ Selmayr, Datenschutzgrundverordnung Art. 58 RN 16). Nach dieser Abgrenzung muss die Nichtbereitstellung von Informationen oder die Auskunftsverweigerung des Adressaten unter Art. 58 Abs. 1 lit. a DS-GVO subsumiert werden.
Gemäß Art. 83 Abs. 5 lit. e DS-GVO kann nach dem Wortlaut nur das Nichtbefolgen einer Anweisung nach Art. 58 Abs. 2 DS-GVO oder

die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO mit einem Bußgeld geahndet werden. Demgegenüber können Verstöße gegen die Zusammenarbeitspflichten, z. B. die Auskunftsverweigerung nach Art. 83 Abs. 4 lit. a i. V. m. Art. 31 DS-GVO geahndet werden.

2. Bewertung

Diese Verortung der fehlenden Informationsbereitstellung oder der Auskunftsverweigerung ist unter den Aufsichtsbehörden umstritten. Zum einen wird Art. 31 DS-GVO von zumindest einem Teil der Kommentarliteratur so verstanden, dass die Zusammenarbeitsverpflichtung von einer Anfrage der Aufsichtsbehörde ausgelöst wird, welche keine Verwaltungsaktqualität haben muss, also eher in Voruntersuchungen zur Sachverhaltsermittlung stattfindet. Eine solche Sachverhaltsermittlung ist jedoch von einer förmlichen Geltendmachung des behördlichen Auskunftsanspruches nach Art. 58 Abs. 1 lit. a DS-GVO zu unterscheiden und in der Folge sind Verstöße gegen die Verpflichtungen auch unterschiedlich zu ahnden.
Zum anderen wird die Inkonsistenz des Auslegungsergebnisses beklagt, da Art. 83 Abs. 4 lit. a DS- GVO i. V. m. Art. 31 DS-GVO einen erheblich niedrigeren Bußgeldrahmen aufweist, als z. B. die Nichtgewährung des Zuganges nach Art. 83 Abs. 5 lit. e DS-GVO i. V. m. Art. 58 Abs. 1 DS-GVO.
Verstöße gegen Art. 58 Abs. 1 lit. a DS-GVO sollten daher wie die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 lit. e oder f DS-GVO gleichmäßig geahndet werden. Daher ist im Rahmen des Art. 83 Abs. 5 lit. e DS-GVO ein Tatbestand für Verstöße gegen eine Anweisung nach Art. 58 Abs. 1 lit. a DS-GVO zu schaffen.

3. Änderungsvorschlag

Änderung des Art. 83 Abs. 5 lit. e DS-GVO:

Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2, Nichtbefolgung einer Anweisung, Informationen bereit zu stellen oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 Buchstaben a, e und f.

Schwerpunktthema Nr. 6 – Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz

I. Art. 46 Abs. 4 i. V. m. Art. 64 Abs. 2 DS-GVO

1. Problemaufriss

Es wird aus dem Gesetzestext nicht klar deutlich, ob bei jeder Verwaltungsvereinbarung, die als Grundlage für internationalen Datentransfer dienen soll und der zuständigen Aufsichtsbehörde gemäß Art. 46 Abs. 3 lit. b DS-GVO zur Genehmigung vorgelegt wird, ein Kohärenzverfahren durchgeführt werden muss. Art. 46 Abs. 4 DS-GVO sieht dies für alle Fälle des Absatzes 3 vor. Art. 64 Abs. 1 DS-GVO erwähnt in lit. e aber nur die Genehmigung von Vertragsklauseln nach Art. 46 Abs. 3 lit. a DS-GVO.
Hintergrund: Seine Stellungnahme zur ESMA/IOSCO Verwaltungsvereinbarung hat der EDSA gemäß Art. 64 Abs. 2 DS-GVO abgegeben. Ob dieses Verfahren in Zukunft für alle Verwaltungsvereinbarungen oder nur für multilaterale Vereinbarungen Anwendung finden soll, wird in der ITES und der COOPESG streitig diskutiert.

2. Bewertung

Es bedarf tatsächlich der Klarstellung, ob auch Verwaltungsvereinbarungen nach Art. 46 Abs. 3 lit. b DS-GVO dem Ausschuss vorgelegt werden müssen. Aus deutscher Sicht ist das der Fall. Allerdings soll hier das Kohärenzverfahren nach Art. 64 Abs. 2 DS-GVO angewendet werden, um dem Ausschuss die Möglichkeit zu geben, bei Verwaltungsvereinbarungen, die nicht die Voraussetzungen des Art. 64 Abs. 2 DS-GVO (Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat) erfüllen, den Antrag auf Stellungnahme abzulehnen.

3. Änderungsvorschlag

Neufassung des Artikels 46 Absatz 4 DS-GVO (4) In Fällen gemäß Absatz 3 Buchstabe a wendet die Aufsichtsbehörde das Kohärenzverfahren nach Art. 64 Abs. 1 Satz 2 Buchstabe e an, in Fällen gemäß Absatz 3 Buchstabe b das Kohärenzverfahren nach Artikel 64 Absatz 2.“

II. Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII

1. Problemaufriss

Als gemäß Art. 97 DS-GVO gesetztes Thema sind die Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII zu behandeln. Konkret stellen sich hier u. a. die Fragen, ob längere Fristen erforderlich sind.

2. Bewertung

Die in der DS-GVO festgelegten Fristen konnten bisher nicht vollumfänglich in der Praxis getestet werden.
Nichtsdestotrotz wurde bereits bei den Anträgen auf Stellungnahme nach Art. 64 Abs. 2 DS-GVO festgestellt, dass eine sachgerechte Behandlung und Diskussion umfangreicherer Themen und schwieriger Einzelfälle durch die Fristen erschwert wird.

3. Änderungsvorschlag

Die Frist des Art. 64 Abs. 3 DS-GVO sollte von acht Wochen auf drei Monate und die Frist des Art. 66 Abs. 4 DS-GVO von zwei auf vier Wochen verlängert werden. Entsprechend müsste dann auch geprüft werden, ob die Geltungsdauer einstweiliger Maßnahmen (Art. 66 Abs. 1 DS-GVO) verlängert wird. Mindestens aber sollte im Kooperations- und Kohärenzverfahren eine Verlängerung aller Fristen um 50 % in Betracht gezogen werden.

III. Art. 64 Abs. 7 DS-GVO

1. Problemaufriss

Die DS-GVO schreibt in Art. 64 Abs. 7 DS-GVO bisher lediglich vor, dass die zuständige Aufsichtsbehörde dem EDSA aufgrund dessen Stellungnahme einen geänderten Beschlussentwurf zur Verfügung stellt (oder mitteilt, dass sie den Beschluss nicht ändern wird). Darauf ist aber keine weitere Rückmeldung des EDSA an die federführende Aufsichtsbehörde mehr vorgesehen.
Zuerst identifiziert wurde dieses Thema im Zusammenhang mit den Kohärenzverfahren zu DSFA- Listen (Art. 64 Abs. 1 lit. a DS-GVO). Vielen Anwendern dieser DSFA-Listen war nicht klar, ob diese nun verbindlichen Charakter haben, nachdem sie gemäß Art. 64 Abs. 7 DS-GVO an die Stellungnahme des EDSA angepasst wurden. Mittler-

weile äußert es sich als großes Problem bei Kohärenzverfahren zu BCR (Binding Corporate Rules), da dort auch Externe (die antragstellenden Unternehmen) betroffen sind. Fällt also eine Stellungnahme des EDSA zunächst negativ aus bzw. werden dort Änderungsbedarfe aufgeführt und ändert das Unternehmen daraufhin seine BCR-Unterlagen (Teil des Genehmigungsentwurfs der federführenden Behörde), erhalten federführende Behörde und Unternehmen keine abschließende Rückmeldung mehr, ob damit den Bedenken des EDSA Genüge getan wurde und ob in der Folge der geänderte Beschlussentwurf verbindlich geworden ist.
Dies ist mittlerweile ein erheblicher Diskussionspunkt mit dem EDSA-Sekretariat. Daher wäre hier eine ergänzende Regelung in Art. 64 DS-GVO für einen vollständigen Abschluss von Kohärenzverfahren erforderlich.

2. Bewertung
Es scheint in der Tat eine Regelungslücke zu bestehen, welches Verfahren ein geänderter Beschlussentwurf nach sich zieht.

3. Änderungsvorschlag
Ergänzung eines zweiten Satzes in Art. 64 Abs. 7 DS-GVO:

Der Ausschuss gibt binnen vier Wochen eine Stellungnahme zu dem geänderten Beschlussentwurf ab. Äußert sich der Ausschuss nicht binnen vier Wochen, so gilt dies als Zustimmung.

Schwerpunktthema Nr. 7 – Direktwerbung

1. Problemaufriss
Mit der DS-GVO sind konkrete Regelungen im nationalen Recht entfallen, die insbesondere Gewichtungen von Interessen vorgesehen haben. Die DS-GVO gibt nur im ErwG 47 DS-GVO einen Anhaltspunkt für die Abwägung: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ In der Praxis stellen sich Fragen, die mit konkreteren Vorgaben des Gesetzgebers besser lösbar wären, z. B.:
Ist die Weitergabe von Kundendaten an Dritte zu Werbezwecken zulässig?

Ist es zulässig, listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen-, oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken (keine Telefon- und Faxnummern, E-Mail-Adresse, Geburtsdatum) für Werbezwecke vorzuhalten und zu nutzen?
Ist die Werbung für wohltätige Zwecke im Ergebnis anders zu bewerten als für wirtschaftliche Zwecke?

2. Bewertung
Direktwerbung betrifft viele Wirtschaftsbereiche und viele betroffene Personen.
Die Traditionen in den Mitgliedstaaten sind unterschiedlich, so dass auch die Erwartungen der Betroffenen, die bei der Interessenabwägung zu berücksichtigen sind, unterschiedlich sein können. Für eine europaweit einheitliche Anwendung sollte der Gesetzgeber deshalb detailliertere Regelungen schaffen.

3. Änderungsvorschlag
Für Direktwerbung sollte der europäische Gesetzgeber in der DS-GVO gesetzliche Vorgaben schaffen, die zumindest die grundsätzliche Gewichtung von Interessen vorsehen.

Schwerpunktthema Nr. 8 – Profiling

1. Problemaufriss
Die Bildung von persönlichen Profilen und deren – kommerzielle und politische – Auswertung sind eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit. Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern. Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DS-GVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur

Schaffung der DS-GVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer detaillierten modernen europäischen Regelung zuzuführen.
Die DS-GVO enthält zwar in Art. 4 Nr. 4 DS-GVO eine Definition des Profiling und der Begriff wird in verschiedenen Erwägungsgründen und Artikeln erwähnt (beispielsweise ErwG 60 DS-GVO, Art. 21, Art. 22, Art. 13 und 14 DS-GVO). Die Profilbildung als solche wird jedoch von den meisten dieser Normen nicht erfasst. Einschränkende Kernregelung ist vielmehr das Verbot der automatisierten Einzelentscheidung mit Erlaubnisvorbehalt (Art. 22 DS-GVO). Das Profiling an sich ist nach geltendem Recht daher vielfach nach den allgemeinen Tatbeständen des Art. 6 DS-GVO zu beurteilen.
Beispielsweise wird Profilerstellung auf Grundlage von Internet-Kommunikationsinhalten und Metadaten u. a. für Werbezwecke von den Unternehmen oftmals nicht als automatisierte Entscheidung angesehen, mit der Folge, dass diese Profilbildung nicht vom grundsätzlichen Verbot des Art. 22 DS-GVO umfasst ist.

2. Bewertung

Die DSK ist der Auffassung, dass vor dem Hintergrund der dargestellten Probleme Änderungsbedarf an den Regelungen der DS-GVO zum Profiling besteht. Ziel der Neuregelungen sollte eine Verschärfung des geltenden Rechtsrahmens sein, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Die betroffenen Personen sollten von einem größeren Maß an Transparenz bezüglich der erstellten Profile profitieren und zugleich eine größere Kontrolle über die Verarbeitung ihrer Daten zur Profilbildung erhalten. Zu diesem Zweck sollte das Verbot der automatisierten Einzelentscheidung in Art. 22 DS-GVO um die Datenverarbeitung zu Zwecken der Profilbildung erweitert werden. Als Rechtsgrundlagen für das Profiling soll – neben einer spezialgesetzlichen Grundlage – allein eine Einwilligung oder ein Vertrag in Betracht kommen. Damit wird sichergestellt, dass ein Profiling nur stattfindet, wenn die betroffene Person sich dessen bewusst ist und damit einverstanden ist.
Die von der Art. 29-Gruppe beschlossenen und vom EDSA bestätigten „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“ geben zwar wichtige Hilfestellung für die datenschutzrechtliche Einordnung

der Profilbildung in der Praxis. Sie können aber eine gesetzliche Regelung nicht ersetzen.

Schwerpunktthema Nr. 9 – Akkreditierung

1. Problemaufriss

In Deutschland gibt es eine Auseinandersetzung zwischen der deutschen nationalen Akkreditierungsstelle und den Aufsichtsbehörden über die Anwendung von Art. 41 DS-GVO. Die deutsche Akkreditierungsstelle vertritt die Auffassung, dass sie auch an Akkreditierungen nach Art. 41 DS-GVO zu beteiligen sei, während die deutschen Aufsichtsbehörden der Auffassung sind, dass die Akkreditierung im Sinne von Art. 41 DS-GVO ausschließlich von den Aufsichtsbehörden durchzuführen ist. Im Verlaufe der Auseinandersetzung hat die Deutsche Akkreditierungsstelle die Aufsichtsbehörden gebeten, sich für eine Klarstellung des Wortlauts einzusetzen.

2. Bewertung

Die deutsche nationale Akkreditierungsstelle schließt aus der Verordnung (EG) Nr. 765/2008, dass sie allgemein für Akkreditierungen in Deutschland zuständig ist. Daher geht sie bisher davon aus, dass auch für die Akkreditierung nach Art. 41 Abs. 1 DS-GVO ein ähnliches Verfahren wie nach Art. 43 Abs. 1 DS-GVO unter Beteiligung der Aufsichtsbehörden durchgeführt wird. Die deutschen Aufsichtsbehörden weisen demgegenüber darauf hin, dass Art. 41 Abs. 1 DS-GVO ausschließlich die Aufsichtsbehörden als akkreditierende Stelle benennt. Der Wortlaut des Art. 43 Abs. 1 Satz 2 DS-GVO unterscheidet sich wesentlich von dem des Art. 41 Abs. 1 DS-GVO. Auch sind im Hinblick auf die Akkreditierung nach Art. 41 Abs. 1 DS-GVO mit Ausnahme von Art. 57 Abs. 1 lit. p DS-GVO (Abfassen und Veröffentlichen der Kriterien) keine konkreten Aussagen in der – im Übrigen im Vergleich zur VO 765/2008 spezielleren – DS-GVO getroffen worden. Nach Auffassung der deutschen Aufsichtsbehörden ist vielmehr davon auszugehen, dass das Wort „Akkreditierung“ in Art. 41 DS-GVO nicht gleichbedeutend mit Akkreditierung im Sinne von Art. 43 DS-GVO und der Verordnung Nr. 765/2008 zu verstehen ist, sondern eine andere Form der „Anerkennung“ darstellt, für die die Verordnung Nr. 765/2008 nicht anwendbar ist.

3. Änderungsvorschläge

In Art. 41 Abs. 1 DS-GVO soll zur Klarstellung vor den Worten „von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde“ das Wort „ausschließlich“ eingefügt werden.

Zusätzlich soll rein klarstellend das Wort „akkreditiert“ gestrichen und stattdessen das Wort „anerkannt“ eingesetzt werden.

Liste weiterer Änderungsvorschläge

Betroffene Vorschrift der DS-GVO	Änderungsvorschlag mit Kurzbegründung
Art. 4	Eine Definition der Anonymisierung fehlt bisher in der DS-GVO. Sie wäre für die Praxis hilfreich. Sie sollte sich an den Vorgaben der „Opinion 05/2014“ zu Anonymisierungsverfahren orientieren.
Art. 13, 14	Die Kataloge der Absätze 2 in Art. 13 und 14 werden aneinander angepasst, indem die Information nach Art. 14 Abs. 2 lit. b DS-GVO auch in Art. 13 DS-GVO nicht in Ansatz 1, sondern in Abs. 2 aufgelistet wird.
Art. 18 Abs. 1	Recht auf Einschränkung der Verarbeitung: Über die unter Art. 18 Abs. 1 lit. a - d DS-GVO aufgezählten Gründe hinaus sollte das Recht auf Einschränkung der Verarbeitung auch in den Fällen bestehen, in denen die an sich gebotene Löschung unterbleibt, weil die Daten gemäß Art. 17 Abs. 3 lit. b DS-GVO lediglich zur Einhaltung von Aufbewahrungsfristen vorgehalten werden müssen.
Art. 21 Abs. 2	Widerspruchsrecht bei Direktmarketing: Durch die Einfügung der Worte „neben dem Widerspruchsrecht nach Abs. 1“ sollte klargestellt werden, dass Abs. 2

	kein Unterfall von Abs. 1 ist, sondern dass der Anwendungsbereich, anders als bei Abs. 1, auch dann eröffnet ist, wenn die Daten nicht auf der Grundlage von Art. 6 Abs. 1 lit. e und f DS-GVO verarbeitet werden.
Art. 24 Abs. 2	Der Wortlaut von Art. 24 Abs. 2 DS-GVO erscheint missverständlich. Er sollte der englischen Fassung wie folgt angeglichen werden: „Einführung“ statt „Anwendung“ und Datenschutz„regelwerke“ statt Datenschutz„vorkehrungen“.
Art. 27	In Art. 27 DS-GVO sollte eine Pflicht zur Veröffentlichung des Vertreters wie in Art. 37 Abs. 7 DS-GVO (Datenschutzbeauftragter) eingeführt werden, da in vielen Fällen unklar ist, ob der Verantwortliche/Auftragsverarbeiter seiner Bestellpflicht nachgekommen ist und wo der Vertreter seinen Sitz hat.
Art. 40 Abs. 4, Art. 41 Abs.1 u. 4	Klarstellung durch Änderungen der genannten Regelungen, ob die Einrichtung einer akkreditierten Überwachungsstelle obligatorisch ist (entsprechend der verabschiedeten Leitlinien des EDSA mit Stand vom 12.02.2019) oder nur fakultativ.

6. Abschlussbericht des Untersuchungsausschusses zum Vorgehen des TLfDI im Fall des Aktenlagers in Immelborn

Die Liegenschaft des ehemaligen Aktenlagers "Ad Acta"
im Gewerbegebiet "Am Bahnhof" in Immelborn.
Foto: TLfDI, im Juli 2013

Mit dem Bericht des von der CDU-Fraktion initiierten Untersuchungsausschusses 6/2 liegt eine umfassende Prüfung und Bewertung des „Falls Immelborn“ vor. Es gibt für das Vorliegen eines missbräuchlichen Amtshilfeersuchens des TLfDI keine Anhaltspunkte. Die Klageerhebung des TLfDI gegenüber dem damaligen Thüringer Innenministerium (TIM) auf Gewährung von Amtshilfe ist aus Sicht des Ausschusses nachvollziehbar und nicht von sachfremden Erwägungen geleitet. Zum Zeitpunkt der Klageerhebung war keine Beräumung des Lagers absehbar. Auch hatte das CDU-geführte TIM ernstlich und endgültig Amtshilfegewährung verweigert, ohne sich auf Verweigerungsgründe berufen zu können. Der Ausschuss erkennt daher an, dass die Erhebung der Klage eine legitime Möglichkeit des TLfDI war, hinsichtlich der rechtlichen und tatsächlichen Situation eine Klärung

herbeizuführen. Anhaltspunkte dafür, dass die Klageerhebung aus anderen als sachlichen Erwägungen erfolgt ist, ergaben sich im Rahmen der Beweisaufnahme nicht.

Nun ist er da! Der Untersuchungsausschuss 6/26 „Aktenlager Immelborn“ legte in der Drucksache Nr. 6/7888 seinen Abschlussbericht auf 1.214 Seiten vor (siehe auch http://www.parldok.thueringen.de/ParlDok/dokument/64557/zwischenbericht-des-untersuchungsausschusses-6-2-aktenlager-immelborn-.pdf).
Verkürzt gesagt sollte der Untersuchungsausschuss aufklären, ob das Vorgehen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach der Entdeckung des Aktenlagers in Immelborn (vergleiche 3. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich Nr. 3.1 mit weiteren Nachweisen) im Juli 2013 rechtmäßig war. Der TLfDI erspart sich an dieser Stelle Ausführungen dazu, ob die Einsetzung eines Untersuchungsausschusses mit einem derartigen Auftrag angesichts der Unabhängigkeit des TLfDI überhaupt zulässig ist.
Über vier Jahre untersuchte der Ausschuss den „Fall Immelborn“. Insgesamt wurden 47 Sitzungen mit zahlreichen Zeugenvernehmungen durchgeführt und alle Unterlagen, die beim TLfDI und anderswo zu diesem Vorgang vorlagen, wurden den Mitgliedern des Untersuchungsausschusses zur Verfügung gestellt. Die Kosten des Untersuchungsausschusses beliefen sich auf insgesamt 907.796 Euro (vergleiche: https://www.mdr.de/thueringen/debatte-um-kosten-von-untersuchungsausschuessen-des-thueringer-landtages-100.html). Nunmehr liegt mit dem Bericht eine umfassende Prüfung und Bewertung vor. Das Vorgehen des Ausschusses und die geprüften Unterlagen können dem Bericht in der angegebenen Drucksache entnommen werden. Der Untersuchungsausschuss kam zu folgenden Ergebnissen:

- Der Untersuchungsausschuss stellte fest, dass die vorgefundenen Unterlagen sich als „in datenschutzrechtlicher Hinsicht relevant“ erwiesen, weil sie personenbezogene Daten enthielten (Rn. 1211).
- Zum Zeitpunkt der Kenntniserlangung des TLfDI befand sich das Aktenlager in einem ungesicherten Zustand (Rn. 1213). Deswegen waren die Akten dem Zugriff unbefugter Dritter ausgesetzt. Die Beweisaufnahme hat ergeben, dass es mehrere Einbrüche in das Aktenlager Immelborn gegeben hatte (Rn. 1299). Der TLfDI hatte bis zur Beräumung 2015 mehrfach Kontakte zu den für die

Sicherungsmaßnahmen zuständigen Stellen bei Polizei und Gemeinde und wies auf die nicht ausreichende Verschlusssicherheit des Gebäudes hin. Für etwaige Versäumnisse bei der Objektsicherung war der TLfDI nicht verantwortlich (Rn. 1216). Bei der Tätigkeit der vor der Entdeckung durch den TLfDI 2013 mit dem Aktenlager befassten Behörden sind in einigen Fällen Versäumnisse festzustellen (Rn. 1426). Für die Räumung des Aktenlagers entstanden bei Privaten Ausgaben, die diese weitestgehend durch den Verkauf des Inventars und Zahlungen der Einlagernden decken konnten. Für den Freistaat Thüringen entstanden durch die Beräumung des Aktenlagers keine Kosten (Rn. 1234f.).

Der Untersuchungsausschuss identifizierte eine Vielzahl von Gründen, die jeweils für sich genommen eine **Verzögerung der Beräumung** zur Folge hatten und in der Zusammenschau ursächlich dafür gewesen waren, dass die endgültige Beräumung des Aktenlagers erst am 2. Februar 2015 begonnen werden konnte (Rn. 1246 ff.):

- Hauptgrund war, dass vor der Bestellung des Nachtragsliquidators keine Beräumung möglich war.
- Offensichtlich konnte der TLfDI die Beräumung mit seinem Personalbestand nicht durchführen (Rn. 1256).
- Durch das Innenministerium wurde jedoch die begehrte Amtshilfe nicht gewährt. Der sich hieraus ergebene Rechtsstreit und das Fehlen der als notwendig erachteten Unterstützung dürften zur Verzögerung der Beräumung nicht unwesentlich beigetragen haben (Rn. 1257).
- Angebote Dritter, die Beräumung vorzunehmen, konnte der TLfDI nicht ohne Weiteres annehmen, ohne Gefahr zu laufen, sich strafbar zu machen (Rn. 1260).

Der TLfDI hat nach der Kenntniserlangung der datenschutzwidrigen Zustände **zwei Bescheide** nach dem Bundesdatenschutzgesetz (BDSG) erlassen, mit der Aufforderung datenschutzrechtliche Zustände herzustellen. Als daraufhin keine Reaktion seitens des Bescheid-Adressaten erfolgte, verschaffte sich der TLfDI zunächst Zugang zu den Räumlichkeiten, um die Akten zu sichten und veranlasste danach die Beräumung des Aktenlagers jeweils im Wege einer Ersatzvornahme.

- Der Bericht stellt fest, dass der TLfDI versucht hat, den datenschutzrechtlich Verantwortlichen nach Aktenlage zu ermitteln. Aus den vorliegenden Informationen habe es sich ergeben, dass

der vormalige Inhaber der Firma Ad Acta zur Verantwortung gezogen werden müsse (Rn. 1354).

- Der TLfDI hat seine Anordnung an den **richtigen Adressaten** gerichtet (Rn. 1450 ff).
- Die öffentliche Zustellung des Bescheides durch den TLfDI erfolgte aufgrund der besonderen Situation aus nachvollziehbaren Gründen, weil die datenschutzrechtliche Gefährdungslage möglichst schnell beseitigt werden sollte und daher Zustellversuche an die zugeklebten Briefkästen für den TLfDI verzichtbar waren (Rn. 1461, 1469).
- Zudem wurde von den Zeugen, die das Objekt nach der Insolvenz und bis Juli 2013 betreten hatten, bekundet, dass sie in dem Gebäude ungeöffnete Briefe auf dem Boden vorgefunden hätten, woraus die Mitarbeiter des TLfDI geschlossen hatten, dass die an die Adresse in Immelborn versandte Post von niemandem mehr zur Kenntnis genommen wurde. Die Beweisaufnahme hat diesbezüglich auch nichts anderes ergeben (Rn. 1358).
- In seiner Stellungnahme zum Abschlussbericht des Untersuchungsausschusses vom 2. August 2018 führte der TLfDI zu dem konkreten, vom Untersuchungsausschuss ermittelten Sachverhalt aus, dass für die Liquidatorenstellung des Zeugen Tischer zum damaligen Zeitpunkt der § 66 Abs. 1 GmbH-Gesetz ausschlaggebend sei, sodass dieser Liquidator kraft Gesetzes wurde und daher über seine Eintragung in das Handelsregister von Amts wegen nicht informiert werden musste (Rn. 1455 ff.). Dieser Auffassung schloss sich der Untersuchungsausschuss an (Rn. 1457).
- Der Untersuchungsausschuss stellte fest, dass die Ersatzvornahme des TLfDI rechtmäßig war (Rn. 1496).

Der TLfDI ersuchte die **Landespolizeidirektion** (LPD) um **Amtshilfe i**m Zusammenhang mit dem Aktenlager Immelborn, da er sich nicht in der Lage sah, die anfallenden Maßnahmen zur Sicherung der Datenbestände mit dem Personalbestand seiner eigenen Behörde bewältigen zu können. Dies ist durch mehrere Zeugen bestätigt worden (Rn. 1504). Nach dem Ausscheiden anderer Alternativen wandte man sich seitens des TLfDI an die LPD in Person ihres damaligen Präsidenten (Rn. 1505).

- Bis zur Kenntnisnahme des Anliegens durch das Thüringer Innenministerium gedachte man seitens der **LPD**, dem zu diesem Zeitpunkt noch nicht förmlich vorliegenden **Amtshilfegesuch** grundsätzlich **stattzugeben** (Rn. 1505).

- Nachdem das förmliche Amtshilfeersuchen am 10. September 2013 bei der LPD eingegangen war, informierte der damalige Präsident das Thüringer Innenministerium am 19. September 2013 mittels Telefax und bat um Zustimmung (Rn. 1522 f.). In einem Begleitschreiben teilte der damalige **Präsident der LP**D mit, dass er **bereit** sei, die beantragte **Amtshilfe zu leisten**.
- Mit Schreiben vom 9. Oktober 2013 lehnte der damalige Präsident der LPD das Amtshilfeersuchen dann jedoch ab. Zur Begründung führte er aus, es handele sich nicht originär um polizeiliche Aufgaben (Rn. 1530).
- Der **Untersuchungsausschuss stellte hingegen fest**, dass angesichts der weiteren Aussagen des damaligen Präsidenten der LPD es aus Sicht des Ausschusses wahrscheinlich ist, dass das **maßgebliche Motiv** der Entscheidung, die **Amtshilfe dann doch noch zu versagen**, war, **nicht gegen den erklärten Willen des Staatssekretärs** im TIM zu handeln (Rn. 1531), denn, so der **Präsident der LPD: „Eine Entscheidung des Innenstaatssekretärs, die er auch im Innenausschuss kundgetan hat, dann als Behördenleiter einer nachgeordneten Behörde mehr oder weniger aufzuheben, das habe ich bisher selten erlebt."** (Rn. 1065).

Also: Ober sticht Unter.

Der Untersuchungsausschuss arbeitete zudem fein heraus:

Vielmehr ist es dem **Thüringer Innenministerium darum gegangen**, so ein Zeuge, **neben den rechtlichen Gründen auch praktische Gründe zu finden, warum die Amtshilfe nicht geleistet werden kann** (Rn. 1076). **Die Frage, ob Amtshilfe überhaupt geleistet werden könne, habe sich gar nicht gestellt** (Rn. 1076).

Obwohl nämlich bei der Bereitschaftspolizei Überstunden kaum beziehungsweise nicht zu verzeichnen waren und folglich Hilfe für den TLfDI möglich war, hat das Thüringer Innenministerium die Bereitschaftspolizei aufgefordert, Argumente zu liefern, die gegen eine solche Unterstützung des TLfDI sprechen sollten (Rn. 1078).

Am 4. Juli 2014 erhob der TLfDI **Klage vor dem Verwaltungsgericht** Weimar gegen den Freistaat Thüringen, vertreten durch den Präsidenten der LPD, auf Aufhebung des ablehnenden Bescheides des Präsidenten sowie des ablehnenden Bescheides des Thüringer Innenministeriums und Gewährung der Amtshilfe.

- Die **Klageerhebung** ist aus Sicht des Ausschusses **nachvollziehbar** und **nicht von sachfremden Erwägungen geleitet**. **Zum**

Zeitpunkt der Klageerhebung war keine Beräumung des Lagers absehbar (Rn. 1565). Auch hatte das TIM ernstlich und endgültig **Amtshilfegewährung verweigert, ohne sich auf Verweigerungsgründe berufen zu können**:

Verbotsgründe, wie sie das TIM skizziert hatte, lagen nicht vor (Rn. 1559). Die **Ablehnung konnte nicht mit dem Verweis auf den Einsatz Privater erfolgen** (Rn. 1560). Auch die Darstellung, es habe eine **ernstliche Gefährdung der Erfüllung eigener Aufgaben der Polizei** gedroht, war nach den Ergebnissen der Beweisaufnahme **nicht haltbar** (Rn. 1560).

Der Ausschuss erkennt daher an, dass die Erhebung der Klage eine **legitime Möglichkeit des TLfDI** war, hinsichtlich der rechtlichen und tatsächlichen Situation eine **Klärung herbeizuführen**. **Anhaltspunkte dafür, dass die Klageerhebung aus anderen als sachlichen Erwägungen erfolgt ist, ergaben sich im Rahmen der Beweisaufnahme nicht.**

Damit ist die mit der Einsetzung des Ausschusses bestehende **Grundfrage**, nämlich, ob der TLfDI die Klage auf Amtshilfe erhob, um dem Innenminister vorsätzlich zu schaden, **eindeutig verneint worden**.

Weitere Einzelheiten und rechtliche Bewertungen können dem Untersuchungsausschussbericht an dem oben genannten Ort entnommen werden.

Zum **Sondervotum** der Mitglieder der CDU-Fraktion im Untersuchungsausschuss erlaube ich mir, die Pressemitteilung der Fraktion DIE LINKE im Thüringer Landtag vom 22. Oktober 2019 zu zitieren: „Der Untersuchungsausschuss ‚Aktenlager Immelborn' hat heute seinen Abschlussbericht beschlossen. Hierzu erklärt der Obmann der Fraktion DIE LINKE im Thüringer Landtag, Rainer Kräuter: ‚Nur dem schnellen und engagierten Handeln des Datenschutzbeauftragten ist es zu verdanken, dass ein riesiges herrenloses Aktenlager in Immelborn letztlich aufgelöst werden konnte und viele hundert Menschen nicht länger fürchten mussten, dass ihre Daten in unbefugte Hände gelangen.'"

Es sei richtig, wenn bei so außerordentlichen Ereignissen nicht lange zugewartet und debattiert, sondern gehandelt wird. Der Vorwurf der CDU, der Datenschutzbeauftragte (TLfDI) habe grob rechtswidrig gehandelt, sei durch umfassende Beweisaufnahme widerlegt.

Vielmehr habe sich im Verlauf der Ausschussarbeit gezeigt, dass es der CDU um eine politische Instrumentalisierung einer Ausnahmesituation ging, um Rot-Rot-Grün und den TLfDI zu diskreditieren. Nach

der Wiederwahl Dr. Hasses zum Datenschutzbeauftragten sei das Interesse der CDU am Untersuchungsausschuss merklich gesunken.

Fazit des TLfDI:

Die Bürgerinnen und Bürger Thüringens haben ihre Schlüsse zu den Vorgängen der verweigerten Amtshilfe in Immelborn, zur Klage des TLfDI gegen das CDU-geführte Innenministerium, zum Untersuchungsausschuss dazu, zur Wiederwahl des TLfDI trotz anonymer Immelborn-Strafanzeige und so weiter längst gezogen.

Der TLfDI bedankt sich bei der Vorsitzenden Frau Henfling dafür, dass das Recht sich in Thüringen durchsetzen konnte.

7. Vorträge und Veranstaltungen

7.1 Der TLfDI informiert! Der TLfDI ist unterwegs! – Presseanfragen zur DS-GVO und Einladungen zu Vorträgen und Veranstaltungen reißen auch 2019 nicht ab!

Eine Großveranstaltung zur KI lockte knapp 200 Gäste nach Erfurt, eine Veranstaltung mit der Verbraucherschutzzentrale „DS-GVO – Besser als ihr Ruf!?“, dazu noch neun Vorlesungen an der Friedrich-Schiller-Universität in Jena und mehr als 100 einzelne Vorträge im Freistaat Thüringen, was für eine arbeitsreiche Bilanz der Öffentlichkeitsarbeit des TLfDI für das Jahr 2019!

Knapp **200** Gäste folgten der Einladung des Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zu einer **Veranstaltung zum Thema Künstliche Intelligenz (KI)** am 1. Juli, darunter **drei** Schulklassen aus Jena, Ruhla und Weimar. Neben dem Grußwort des Ministers für Digitales, Herrn Wolfgang Tiefensee, bereicherten unter anderem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Herr Ulrich Kelber, und die Abgeordnete des Landtags Frau Dorothea Marx die Veranstaltung durch ihre Vorträge. Der BfDI betonte, dass die EU-Datenschutz-Grundverordnung vor Auswüchsen der KI angemessen schützt. Frau Marx verwies auf die Gefahren der KI bei Wahlen durch Wählermanipulationen. Dass selbst scheinbar geschützte Internetseiten für Schüler getrackt werden, stellte Frau Prof. Jana Dittmann von der Uni Magdeburg dar. Reinhard Karer, Pressesprecher des Deutschen Forschungsinstitutes für KI, hob natürlich die Weiterentwicklung der künstlichen Intelligenz im positiven Sinne hervor. Jay Tuck, US-Sicherheitsexperte und Buchautor, der die Veranstaltungsreihe des TLfDI bereits das zweite Mal durch seine effektvollen Vorführungen mitgestaltete, malte in etwas düsteren Farben, dass die KI schon heute den Menschen übertrifft und qualifizierte Jobs übernehmen wird. Für seinen Beitrag erhielt er Standing Ovations von den Schülerinnen und Schülern! Zwei berufene Schüler beteiligten sich aktiv an der abschließenden Podiumsdiskussion und standen dem Publikum Rede und Antwort. Eine spannende und kontroverse Veranstaltung, die auch das Publikum bis zum Ende gefesselt hat. Fortsetzung folgt! 2020 ist eine Großveranstaltung zu P R O F I L I N G geplant.

Foto: TLfDI

Die **Kooperationsveranstaltung „Datenschutz-Grundverordnung – Besser als ihr Ruf!?“ mit der Verbraucherschutzzentrale Thüringen** im April 2019 beschäftigte sich unter anderem mit folgenden Fragen der Verbraucher: Darf mein Hausarzt mich noch mit meinem Namen ins Behandlungszimmer rufen? Braucht unser Fußballverein einen Datenschutzbeauftragten? Was nützt mir der „Papierwust“, den ich nun zu jedem Vertrag erhalte? Müssen bald die Klingelschilder an Wohnblocks abgeschraubt werden? Denn seit dem 25. Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DS-GVO). Sie sollte eigentlich die entsprechenden Grundsätze und Normen in der Europäischen Union harmonisieren. Harmonie hat sich indes noch nicht eingestellt. Für viele Verbraucherinnen und Verbraucher existieren Unsicherheiten, sind Fragen offen – nicht zuletzt die Kernfrage: Was nützt mir die DS-GVO? Die Verbraucherzentrale Thüringen und der TLfDI haben aktuelle Fälle und Aufreger diskutiert und rechtlich eingeordnet.

© Oliver Boehmer - bluedesign®- Schilder Gelb -fotolia.com

Der TLfDI informiert!
Weiterhin gab es eine sehr hohe Nachfrage nach Vorträgen und Vorlesungen zum Datenschutz auch im Berichtsjahr 2019:

Die Anfragen zu Schulungen durch den TLfDI sind auch 2019 nicht abgerissen. Über 100 Vorträge an Universitäten, in Pflegeeinrichtungen oder in Ortsverbänden der Vereine, die Neuerungen der DS-GVO betreffend, wurden von Mitarbeitern des TLfDI umgesetzt. Um so viele Unternehmerinnen und Unternehmer, Vereinsvorsitzende und andere Datenschutzbeauftragte wie nur möglich zu erreichen, gab es auch in diesem Jahr die Möglichkeit, an Sammelvorträgen in der Industrie- und Handelskammer Erfurt teilzunehmen. Die Lehrerfortbildung wurde ebenfalls großgeschrieben.

Auch bei Veranstaltungen in der ganzen Bundesrepublik war der TLfDI ein gefragter Redner und Podiumsgast, von „A“ wie „Autorecht“ über „D“ wie „didacta“ zu „I“ wie „IT-Sicherheit und IT-Kongress“ über „K“ wie „Kammergespräch“ und „Konferenz Bildung und Digitalisierung“ bis „V“ wie “ver.di“ und „Verwaltungsgerichtsbarkeit“. Hier standen vor allem die Fragen im Vordergrund, wie die Aufsichtsbehörde die DS-GVO umsetzt und die Kooperation der Aufsichtsbehörde mit der Wirtschaft!

Im Jahr 2019 hielt der TLfDI an der Rechtsfakultät der FSU Jena sieben Vorlesungen im Sommersemester und zwei Blockvorlesungen im Wintersemester. Er berichtete über seine Behörde und deren Befugnisse nach dem neuen Datenschutzrecht, gefolgt von einem kurzen historischen Abriss zur Entwicklung des Datenschutzrechts bis hin zur Datenschutz-Grundverordnung (DS-GVO). Dann sezierte er die neuen Regelungen der DS-GVO. Die Vorlesungen waren angereichert mit Fällen, Clips und Grafiken sowie aktuellen Themen (zum Beispiel selbstfahrende Fahrzeuge, Medienkompetenz an (Hoch-)Schulen, Arbeit 4.0, Künstliche Intelligenz) und datenschutzrechtlichen Skandalen des Tages. Datenschutz soll und kann auch Spaß machen! Das war das Ziel. Für diese Veranstaltung war keine Anmeldung erforderlich, so dass jeder daran teilnehmen konnte. Fortsetzung folgt auch hier! Die Planungen für das Sommersemester 2020 an der FSU in Jena laufen bereits.

Stichwortverzeichnis

Abgeordneter....2.3
Abwesenheitsliste....3.21
Administrator....3.23
Adressbuch....4.17
Adressdaten....3.34
Adressfeld....3.20
Akteneinsicht....4.21, 4.2, 3.32, 3.8
Aktenlager....6
Algorithmen....2.2
Ältestenrat....2.3
Amt für Verfassungsschutz....2.4
Amtsblatt....3.10
Amtshilfe....6
Amtshilfegesuch....6
Analysetool....3.26, 1.1
Analysetools....2.12
Anhörungsverfahren....1.2
Anleger....4.21
Anmeldung....4.16
anonyme Nummernvergabe....3.13
Anonymisierung....4.3, 3.14, 2.2
Anordnung....1.2
Anordnungsbescheid....4.13
Anti-Terror-Datei....2.4
Anweisung....2.4
Anwohnerparkplakette....3.16
App....2.15
Arbeitgeber....4.9, 4.8
Arbeitgeberverband....3.20
Arbeitnehmer....4.8
Archivgesetz....3.3
Arzt....4.16, 3.37, 3.36
Arztausweis....3.37
ärztliches Gutachten....3.15
Arztpraxis....4.15, 3.22
Assetmanagement....3.23
Aufbewahrungsfrist....3.3

aufschiebende Wirkung....2.4
Auftragsverarbeitungsvertrag....3.26, 2.15
Ausbildungsbetrieb....3.22
Auskunft....4.13, 3.8, 3.4, 2.1, 1.2
Auskunftsanspruch....3.32
Auskunftsrecht....3.11, 3.7, 2.5
Auskunftssperre....3.34, 3.9
Aussonderung....3.2
Ausstellung....4.20
Ausweispflicht....3.16
Auszubildende....3.22
Authentisierung....3.36
Authentizität....2.7
Bank....3.42, 3.40
Bankdaten....4.4
Beanstandung....2.4
Befugnisse....2.4
behördlicher Datenschutzbeauftragter....3.4
Beifahrer....3.5
Beihilfe....3.24
Beihilfeberechtigte....3.24
Beihilfestelle....3.24
berechtigte Interessen....4.18, 3.22, 2.1
Bereitschaftspolizei....6
Berichtigung....2.5
Berufsgeheimnis....4.14
Berufskraftfahrer....3.15
Berufsschule....3.22
Beschäftigte....4.8, 3.7
Beschäftigtendaten....4.9, 3.21
Bescheid-Adressat....6
Beschwerde....2.15, 2.4, 2.1, 1.2, 1.1
besondere Kategorien personenbezogener Daten....4.17, 3.37
besondere Kategorien von Daten....4.11, 3.12
betrieblicher Datenschutzbeauftragter....3.33
Betriebskosten....3.33
Betroffenenrecht....2.5
Beweisaufnahme....6
Beweisverwertungsverbot....3.5
Bewerbung....4.6

biometrische Analyse 2.9
biometrische Sensoren 2.9
BKA 3.34
Blitzerfoto 3.5
BSI 3.36
Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.37
Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI) 2.8
Bundesnetzagentur (BNetzA) 2.8
Bußgeld 4.21, 4.3, 2.16, 2.9, 1.2, 1.2
Bußgeldstelle 3.5
Bußgeldverfahren 4.4, 3.17, 3.5, 1.2
Café 4.5
Cloud 3.28
Cloud-Dienste 1.1
Cloudspeicher 2.15
Cyber-Kriminalität 3.38
Datenabgleich 3.40
Datenethikkommission der Bundesregierung 2.2
Datengeheimnis 4.3
Datenminimierung 2.15, 2.2
Datenpanne 3.38, 3.31, 3.13, 2.16, 2.10, 1.2, 1.2, 1.1
Datensatz 2.5
Datenschutz durch Technikgestaltung 3.23
Datenschutzbeauftragter 4.1, 2.6
Datenschutzerklärung 3.26, 1.1
Datenschutz-Folgenabschätzung 3.26, 3.24, 3.2, 2.9, 2.6, 1.1
Datenschutzkontrolle 2.3
datenschutzrechtliche Voreinstellungen 3.23
Datensicherheitsmaßnahmen 2.7
Datensparsamkeit 4.4
Datenübermittlung 4.18
Datenübermittlung in das Ausland 3.41
Diagnose 3.24
didacta 7.1
Diebstahl 1.2
Dienstplan 3.21
digitale Schul- und Verwaltungsplattform DigLu - Digitales Lernen 3.28
Digitalisierung 3.2

DigitalPakt 3.25
Digitalstrategie Thüringer Schule (DiTS) 3.25
Direkterhebung 3.39
Diskriminierung 2.2
Dokumentation 1.1
Dokumentenmanagementsystem 3.2
Dritterhebung 3.39
eAkte 3.2
E-Government 3.2
Ehrenamt 4.17
Eigentümerwechsel 4.4
Einkommensverhältnisse 4.19
Einwilligung 4.20, 4.15, 4.9, 4.7, 4.4, 4.2, 3.42, 3.28, 3.27, 3.26, 3.22, 3.12, 2.12
Einwohnermeldeamt 3.34
elektronische Antragstellung 3.24
elektronische Gesundheitskarte 3.37
elektronische Patientenakte 3.37
elektronischer Arztbrief 3.37
elektronisches Fax 3.20
elektronisches Magazin 3.2
elektronisches Patientenpostfach 3.37
ELSTER 3.41
Eltern 4.19, 3.33, 3.32, 3.29, 3.28, 3.27, 3.25
E-Mail 4.14, 4.6, 3.41, 3.38, 3.30, 3.29, 3.25
E-Mailadresse 1.2
Empfänger 2.5
Ende-zu-Ende-Verschlüsselung 3.30, 3.29
Energieversorger 4.7
Entschließung 2.2
Erkennung von Gesichtern 2.2
Ersatzvornahme 6
Europäischer Gerichtshof (EuGH) 2.8
externe Dienste 3.26
Facebook-Fanpage 2.13
Fahreignungsvoraussetzungen 3.15
Fahrerlaubnisbehörde 3.15
Fahrzeug 4.9, 3.5
Falschversendung 2.16
familiäre Tätigkeit 4.18

FAQs 3.30
Faxgerät 3.20
Faxnummer 4.11
Fehlzeiten 3.22
Finanzbehörde 4.10
Finanzministerium 3.24, 3.2
Firmenwagen 4.9
Fondsgesellschaft 4.21
Formatkonvertierung 3.2
Forschungsprojekt Sicherheit und Kriminalität in Deutschland (SKiD) 3.34
Foto 4.20, 4.15
Fotograf 4.20
Fraktion 2.3
Freiwilligkeit 4.9, 4.7
Freizeit 4.5
G10-Kommission 2.3
Gastronomie 4.5
Gebühren 3.32
Geldbuße 3.39, 1.2
Geldwäschegesetz 4.10
Gemeinde 6, 3.33
Gemeinderat 3.14
Gemeinderatssitzung 3.12
Gemeinderatswahl 3.10
Gericht 3.6
Gerichtsverfahren 3.6, 2.4
Geschäftsgeheimnis 2.5
Gesellschaft für Telematik 3.37
Gesundheitsdaten 4.16, 3.37, 3.24, 3.21
Gläubigeradressen 4.2
Gleichwellenfunkkanal 2.4
Gmail 2.8
Google 3.31, 2.8
Google Analytics 3.26, 2.12
Google Formulare 2.14
Google-Suche 3.31
GPS-Daten 4.9
GPS-Überwachung 1.2
Großraumbüro 3.13

Gruppenauskunft 3.34
Hackerangriff 2.4
Halt- und Parkverstöße 3.17
Hambacher Erklärung 2.2
Handelsregister 6
Handreichung 2.6
Handwerkskammer 1.1
Hasso-Plattner-Institut (HPI) 3.26
Hausaufgaben 3.26
Haushalts-, Kassen- und Rechnungswesen des Bundes (HKR-Verfahren) 3.19
Haushaltsprivileg 4.17
Haushaltsrecht 3.33
häusliche Pflege 3.27
Hilfsmerkmale 4.8
hohes Risiko 2.9, 2.6
Hundesteuer 3.18
Identifizierungsverfahren 3.37
Identitätsdiebstahl 2.16
Identitätsfeststellung 3.16
Immelborn 6
Immobiliengewerbe 1.2
Immobilienmakler 4.3
Immobilienverkauf 4.18
Industrie- und Handelskammer 7.1, 1.1
Information an den Betroffenen 3.4
Informationspflicht 4.8, 3.39, 3.19, 1.2
Informationsveranstaltung 1.1
Innenministerium 6
Insolvenz 4.21
Insolvenzgericht 4.21
Insolvenzverfahren 4.13, 4.2
Insolvenzverwalter 4.21
Integrität 3.2, 2.7
Interessenabwägung 4.5, 4.2
Interessenkonflikt 4.1
interkommunaler Vergleich 3.14
Internet 4.20, 4.17, 3.31
Internetauftritt 3.31
Internetportal 4.3

IP-Adresse 3.26
IT-Administrator 4.1
IT-Sicherheitsbeauftragter 4.1
IT-Sicherheitskonzept 3.24
IT-Sicherheitsmaßnahmen 2.7
Jahresabrechnung 4.4
JI-Richtlinie 2.4
Jugendamt 4.19, 3.39
Justiz 3.6
Kalender 3.21
Kamera 4.5, 2.15
Kanzlei 4.14
Kategorien von personenbezogenen Daten 3.39, 2.5
Kfz-Zulassungsstelle 3.13
Kind 4.19, 3.33, 3.31
Kinder beruflich Reisender 3.28
Kindertageseinrichtung 3.33
KI-Systeme 2.2
Kita 3.33
Klage 6, 2.4
Klardaten 3.26
Klassenbuch 3.31
Klinik 3.37
kommunale Satzung 3.12
Kommunalwahl 3.9, 1.1
Kommune 3.18, 3.16, 3.12, 3.11, 3.10, 2.4, 1.1
Kommunikationsnetze 2.8
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) 2.13, 2.9, 2.2
konkrete Gefahr 4.5
Kontrollen 2.4
Kontrolltätigkeit 1.1
Kopie 2.5
Kopie der Daten 4.13
Kopplungsverbot 4.7
Kostenträger 3.37
Kostentragungspflicht 4.13
Krankenhaus 3.38, 3.36
Krankheit 3.21, 3.15
kryptographische Speicherverfahren 2.10

Kultusministerkonferenz (KMK) 3.28, 1.1
Kundenberatung 3.42
künstliche Intelligenz 2.2
Künstliche Intelligenz 7.1
Künstliche Intelligenz 1.1
Kunsturhebergesetz 4.20
Kuvertierfehler 2.16
Landesamt für Statistik 4.8
Landeskriminalamt 2.4
Landespolizeidirektion (LPD) 6
Landespolizeiinspektion 3.4
Landtag 3.1
Langzeitspeicherung 3.2
Lehrer 3.30, 3.29, 3.26, 3.25
Lehrplan 3.28
Leistungsbewertung 3.28
Leistungsmissbrauch 3.40
Lernplattform 3.26
Lesebestätigung 3.41
Liveübertragung 3.27
Log-Dateien 2.7
lokales Netzwerk 2.15
Löschantrag 3.31
Löschfrist 2.14
Löschprotokoll 3.12
Löschung 4.10, 3.4, 2.5
Mandantenstammblatt 4.21
Mandat 4.2
Mandatsakquise 4.21
Mandatsausübung 4.14
Medienkompetenz 7.1
Medikationspläne 3.37
Meldepflicht 2.16, 2.8
Melderegister 3.9
Melderegisterauskunft 3.34
Meldung einer Datenpanne 4.11
Messenger 3.29
Messenger-Dienst 2.8
Microsoft 2.11
Mieter 4.3

Mieterliste 4.3
Mitarbeiter 4.15, 4.9, 3.23
Mitarbeiterüberwachung 3.23
Museum 3.35
MVZ 4.16
Nachtragsliquidator 6
Name des Zeugen 3.17
nationale Sicherheit 2.1
nicht-öffentliche Sitzung 3.14, 3.12
Niederschrift 3.12
Normenklarheit 3.3
Notar 3.8
Noten 3.22
Notenverwaltung 3.30
Notfall 3.31
Notfalldatensatz 3.37
Objektsicherung 6
öffentlich zugängliche Quelle 3.39
öffentliche Bekanntmachung 3.10
öffentliche Sicherheit und Ordnung 3.16
öffentliche Stelle 2.14
öffentliche Zustellung 6
öffentlichen Bekanntmachung 3.9
öffentlicher Bereich 2.1
Öffentlichkeit 3.6
Online-Dienst 2.10
Online-Petition, ... 3.1
Ordnungsbehörde 3.17
Ordnungswidrigkeitenverfahren 4.21
Orientierungshilfe 2.12
Ortschronik 4.20
ortsübliche Bekanntmachung 3.12
Ortungssystem 4.9
Over-the-top-Dienst (OTT) 2.8
Pachtvertrag 4.12
parlamentarische Datenschutzordnung 2.3
parlamentarische Kontrollkommission 2.3
parlamentarische Tätigkeit 2.3
Partei 4.11
Passwort 3.36, 2.10

Passwortlänge 2.10
Patient 4.16, 3.37, 3.36
Person der Zeitgeschichte 4.20
Personalausweis 4.10, 3.35, 3.16, 3.7
Personalausweisgesetz (PAuswG) 3.16
Personalausweiskopie 4.10
Personaldaten 4.6
Personalrat 3.23
persönlicher und familiärer Bereich 4.17
Petition 3.1
Pfandmittel 3.35
PGP-Verschlüsselung 3.29
Phishing-Mails 3.38
Pilotprojekt 3.28
politische Meinung 4.11
Polizei 6, 3.34, 3.7, 3.4, 2.4
Positionspapier 2.9, 2.2
Posteingang 1.2
Postgeheimnis 4.7
Presse 3.14
Presseanfragen 7.1
privater PC 3.30
Profiling 7.1, 1.1
Prüfschema 2.11
Prüfungsbericht 3.14
Pseudonymisierung 3.26, 2.2
Publikum 4.20
Qualifikation 4.1
Quelle der Daten 3.39
Rechenschaftspflicht 2.2
Rechnungsprüfung 3.33
Recht auf Beschwerde 3.39
Rechtsanwalt 4.21, 4.13, 4.2, 3.22, 1.2
Rechtsbehelf 2.4
Rechtskraft 2.4
Recyclingunternehmen 4.10
Regelschule 3.31
Rettungsdienstverband 2.4
Revisionsfähigkeit 2.7
Rezepte 3.24

Richtlinie über den neuen europäischen Kodex für die elektronische Kommunikation (EKEK) 2.8
Richtlinie über die Aufbewahrung von Akten und sonstigem Schriftgut in der Verwaltung des Freistaats Thüringen 3.3
Risiko 2.7
Sanktion 1.2
SATELIT 3.36
Satzung 3.18
Schaukasten 4.12
Schlaganfall-Zentrum 3.36
Schnittstelle 3.26
Schriftgutstruktur 3.2
Schulamt 3.31
Schul-Cloud 3.26, 3.25
Schuldner 3.19
Schule 3.32, 3.31, 3.28, 3.27, 3.26, 3.25, 1.1
Schüler 3.30, 3.29, 3.28, 3.27, 3.26, 3.25, 3.22
Schulleiter 3.31
Schulpflicht 3.28
Schultagebuch 3.28
Schulungen 7.1, 1.1
Schulungsdaten 4.14
Schutzniveau 2.7
Schweigepflicht 3.8
Selbstbezichtigung 2.16
Selbstdatenschutz 3.25
Sicherheit der Verarbeitung 2.10
Sicherheitskonzept 3.37, 3.26
Sicherheitszertifizierung 3.37
Sicherungsmaßnahmen 6
Signalerkennung 2.2
Signalübertragung 2.8
Sitzungsprotokoll 3.12
Smart City 1.1
Smartphone 2.15
sofortige Vollziehbarkeit 4.13
Sozialbehörde 3.40
soziale Netzwerke 4.17
Speicherbegrenzung 2.15
Speicherdauer 2.15, 2.5

Sportveranstaltung 4.20
Spracherkennung 2.2
Staatssekretär 6
Stadtverwaltung 3.14
Stammdaten 3.40, 3.28
Standard-Datenschutzmodell (SDM) 2.6
Statistik 4.8, 3.23, 1.2
Steuerdaten 3.41
Strafverhandlung 3.6
Straßenausbaubeitrag 2.1
Straßenverkehr 3.15
Straßenverkehrs-Ordnung 3.16
Supervisor 3.23
symmetrischer Verschlüsselungsalgorithmus 2.10
technische und organisatorische Maßnahmen ... 4.16, 2.9, 2.6, 2.4, 2.2
Telefax 4.11, 3.20
Telefonserver 3.23
Telekommunikationsdienst 2.8
Telemedien 2.12
Telemedizin 3.36
Telemetriedaten 2.11
Telepräsenzavatare 3.27
Terrasse 4.5
Thüringentag 3.16
Thüringer Datenschutzgesetz 2.4, 2.1
Thüringer Landtag 2.3
Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) . 3.28
Thüringer Ministerium für Inneres und Kommunales 3.3
Thüringer Pilotschulen 3.26
Thüringer Rechnungshof 3.14
Thüringer Schul-Cloud 1.1
Thüringer Schulgesetz (ThürSchulG) 3.28
Tonmitschnitte 3.12
Tracking 3.26
Trainingsdaten 2.2
Transparenz 2.14, 2.13, 2.7, 2.5, 2.2, 1.1
Transportverschlüsselung 3.29
Über-/ Unterordnungsverhältnis 3.22
überörtliche Prüfung 3.14
Überstunden 6

Umfrage 3.34, 1.1
Unabhängigkeit des TLfDI 6
Universitätsklinikum Jena 3.36
Unterhalt 4.19
Unterhaltsvorschuss 4.19
Unternehmen 1.1
Unternehmensberatung 4.14
Unterricht 3.28, 3.27
Unterrichtsfach Informatik und Medienbildung 3.25
Urheberrecht 2.5
Urkunde 3.8
USB-Stick 3.30
Verarbeitungszwecke 2.5
Verbot 2.4
Verbot mit Erlaubnisvorbehalt 2.1
Verdienststatistik 4.8
Verein 4.20, 4.12
Verfügbarkeit 2.7
Verkehrsüberwachungsmaßnahme 3.5
Vernichtung 3.36
Veröffentlichung im Internet 3.12
Veröffentlichung von Protokollen 4.12
Verpixelung 3.5
Verschlüsselung 4.14, 4.6, 3.30
Verschlusssicherheit 6
Versichertenstammdaten 3.37
Versicherungsmakler 1.2
Versicherungsnummer 4.8
Versorgungsbezügeempfänger über das Thüringer Antragssystem für Verwaltungsleistungen (ThAVEL) 3.24
Vertrag 4.10
Vertraulichkeit 2.7
Verwalter 4.4
Verwaltungsakt 2.4
Verwaltungsaufgaben 2.3
Verwaltungsgericht 6
Verwandte 4.18
Verwarngeldangebot 3.17
Verwarnung 3.31, 2.4
Verzeichnis von Verarbeitungstätigkeiten 2.15, 2.4

Videokamera 2.9
Videoüberwachung 4.17, 4.5, 2.15, 2.9, 2.4, 1.2, 1.1
Vier-Augen-Prinzip 3.23
Vollmacht 4.21, 4.2
Vollstreckung 3.19
Vollstreckungsverfahren 3.19
Vorbesitzer 3.18
Vordruck 3.40, 3.24
Vorgesetzter 3.23
Vorlesung 7.1
Vor-Ort-Kontrolle 3.31, 3.26
Wahlkreismitarbeiter 2.3
Wahlleiter 3.10, 3.9
Wahlvorschlag 3.10
Wartezone 3.13
Wartung 3.36
Webangebot 3.26
Webmail 2.8
Webseite 1.1
Website 3.1
Werbung 4.21, 4.7, 4.2
Widerruf der Einwilligung 4.15, 4.7
Widerspruch 2.1
Windows 10 ..... 2.11
Wohnungseigentümergemeinschaft 4.4
Wortprotokoll 3.12
xdomea 3.2
Zeugnis 3.30, 3.28
Zugangssicherung 2.10
Zugriffsrechte 4.6
Zuständigkeitsregelung 2.8
Zustellung 3.20, 2.4
Zustellversuch 6
Zweckänderung 3.19
Zweckbindung 4.4, 2.2
Zweckerreichung 4.10
Zwei-Faktor-Authentifizierung 2.10