



3. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

3. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Be- reich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2016 bis 31. Dezember 2017
Zitiervorschlag: 3. TB LfDI Thüringen

Der 3. Tätigkeitsbericht steht im Internet unter der
Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Dezember 2017

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

Inhaltsverzeichnis

Vorwort 12
1	Schwerpunkte im Berichtszeitraum..... 16
2	Der betriebliche Datenschutzbeauftragte 19
2.1	Europäische Datenschutz-Grundverordnung: Unternehmen fragen – TLfDI informiert 19
2.2	Darf ein IT-Mitarbeiter gleichzeitig betrieblicher Datenschutzbeauftragter sein? 21
2.3	Darf ein IT-Sicherheitsbeauftragter gleichzeitig Datenschutzbeauftragter des Unternehmens sein?..... 24
2.4	Zu viele auf einmal: Bestellung einer Rechtsanwalts- Partnerschaft zum Datenschutzbeauftragten 26
2.5	Bestellung eines Datenschutzbeauftragten 28
2.6	Die Europäische Datenschutz-Grundverordnung kommt – und die Unternehmen machen sich so ihre Gedanken 31
2.7	Einbruchdiebstahl in der Kita 33
3	Umgang mit Kundendaten..... 36
3.1	Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig! 36
3.2	Nerviges Meinungsforschungsinstitut 37
3.3	Daten-Theater 39
3.4	Der Anwalt als Datenschleuder? 41
3.5	Reparatur inklusive Datenverlust – wer richtig liest, erspart sich viel Ärger..... 43
3.6	Datenerhebung zur Beitreibung rechtmäßiger offener Forderungen ist kein Datenschutzverstoß..... 45
3.7	Bewerbung erfolglos – Daten löschen! 47
3.8	Hotelinsolvenz: Gehören die Kundendaten dem neuen Eigentümer?..... 48
3.9	Das Probeabonnement einer Zeitung als Türöffner für Werbeattacken 52
3.10	Baumarkt verlangt Adressangabe beim Umtausch 54

3.11	Versteckte Einwilligungserklärung.....	56
3.12	Pkw-Stellplatz gegen Ausweiskopie – was ist in der Mieterselbstauskunft zulässig?	58
3.13	Bestattungskosten: Datenschutz kein Kostenschutz ..	60
3.14	Unzulässige Kopie des Personalausweises – keine Bombenidee	61
3.15	Ver(un)sicherung	64
3.16	Einmal hin, einmal her – Versicherungsvermittlung ist manchmal schwer	66
3.17	Seminararbeit im Netz: nur ohne Personenbezug	67
3.18	Welche Mitgliederdaten darf ein Verein erheben und an seinen Dachverband weitergeben?	68
3.19	Zahlartensteuerung – nein, danke!	73
3.20	Der TLfDI macht viel – aber nicht alles	75
3.21	Pressefreiheit versus Datenschutz?	76
3.22	Wie oft muss man der Hausbank den Personalausweis vorlegen?	78
3.23	Wenn die Hausbank keine Auskunft erteilt	79
3.24	Frage eines Software-Entwicklers: Veröffentlichung von Vertretungsplänen sowie Stundenplänen innerhalb einer App für Schulen	80
3.25	Mitgliedsbeiträge am schwarzen Brett?	81
3.26	Der Übergang von Kundendaten bei Unternehmensverkäufen	82
3.27	Datenschutz für Pseudonym?	85
3.28	Bürgerinitiative ratlos – der TLfDI kann helfen	86
3.29	Aktenlager überall	88
3.30	Umfrage des TLfDI – Thüringer Unternehmen zeigen sich hinsichtlich Datenschutzerfordernungen höchst vorbildlich	89
3.31	Weitergabe von Kundenverbrauchsdaten durch Versorgungsunternehmen	95
3.32	Schrott sammeln = Daten sammeln? Fortsetzung II ..	97
3.33	Handy als Navigator im Einkaufszentrum – beim TLfDI läuten die Alarmglocken	98
3.34	Öffentlich zugänglich aufgestellte Container mit Akten eines Steuerbüros in Gera	100
3.35	Onlineshops: Kreditkartendaten frei Haus?	102
3.36	Datenschutz auch beim Schornsteinfeger	105

3.37	Datenübermittlung von Makler zu Makler – Der TLfDI bezieht Stellung!.....	106
3.38	Digitale Unterschriften versus Datenschutz.....	108
3.39	Schreddern? – Aber richtig?	109
3.40	Hilferuf eines Vereins aus dem datenschutzrechtlichen Dickicht	111
3.41	Vereinsberatung.....	114
3.42	Herrenlose Akten eines Bauunternehmers.....	115
3.43	Nachhilfe: Bürger erhält Auskunft	117
3.44	Keine Lastschrift ohne Daten	118
3.45	Jeder kennt jeden – Hausverwaltung gibt Daten weiter	120
3.46	Ich bin du, du bist ich?.....	123
3.47	Geheimnis: Akten einer Steuerberatungskanzlei	124
3.48	TLfDI kontrolliert Weihnachtsmann ;-)	126
4	Datenschutzkonformität von unternehmensinternen Unterlagen	128
4.1	Datenschutz auch bei Korruptionsbekämpfung.....	128
4.2	Datenschutz im Sportverein – was dürfen SV, FC und Co.?.....	131
4.3	Da wird der Hund in der Pfanne verrückt.....	133
4.4	Falscher Adressat TLfDI	137
4.5	Datenschutz bei der App-Entwicklung	138
5	Meldungen nach § 42a.....	140
5.1	Leaks	140
6	Videüberwachung.....	143
6.1	„1984“ war gestern!.....	143
6.2	Meldungen nicht nur von Wildkameras.....	145
6.3	Selbstbedienungsladen ohne Personal, aber mit problematischer Überwachungstechnik?	147
6.4	Rundumüberwachung einer Wohnungsanlage	150
6.5	Video versus Vandalismus – Videogaga?	154
6.6	Pizza mit Draufsicht – Videogaga 1	156
6.7	Big Brother auf dem Marktplatz – Videogaga 2.....	159
6.8	Videüberwachung auf Firmengelände – Videogaga 3	161
6.9	Tanken mit Stummfilm – Videogaga 4.....	164

6.10	Smart-Home-Präsentation: inklusive Videoüberwachung.....	166
6.11	Video für Baufortschritt – kein Fortschritt – Videogaga 5.....	167
6.12	Videoüberwachung der Insolvenzmasse.....	169
6.13	Der (Tür)Spion, der die Nachbarn nicht liebte; Videogaga 6.....	170
6.14	Man kann den Pelz nicht waschen, ohne sich nass zu machen: Videogaga 7	174
6.15	Bei Klingeln Aufnahme: BDSG?	175
6.16	Fenster zum Hof	176
6.17	Auskunftsverweigerungs(un)recht.....	179
6.18	Der abgeschottete Nachbar	180
6.19	Postkartenmotiv „Videokamera“	184
6.20	Videoüberwachung eines öffentlichen Raumes der Stadt Rudolstadt durch Privatperson.....	185
6.21	Videoüberwachung nicht über den Maschendrahtzaun hinaus?	187
6.22	Videoüberwachung auf eigenem Grundstück zulässig?	190
6.23	Achtung: Im Vogelhaus nistet eine Kamera! – Videogaga 8.....	191
6.24	Dome	194
6.25	Wanderer zeigen Bein: Videogaga 9	196
6.26	Kamera im Mehrfamilienhaus beliebt: Videogaga 10	197
6.27	Störung des Hausfriedens durch Videoüberwachung – Videogaga 11.....	198
6.28	Rund um die Uhr ein Blick ins Unternehmen – Videogaga 12.....	202
6.29	Campingplatzatmosphäre – Videogaga 13	204
6.30	Zeugnisverweigerungsrecht schließt Vorgehen des TLfDI nicht aus	205
6.31	Videoüberwachung – der TLfDI hilft, wenn er weiß, wo: Videogaga 14.....	206
6.32	Hotelgäste und Mitarbeiter pausenlos auf Video? Videogaga 15.....	208
6.33	Grundstücksgrenze = Ende der Beobachtungsbefugnis	209
6.34	Und weg ist die Attrappe: Videogaga 16.....	210

6.35	Kamera als Abschreckung zulässig?: Videogaga 17	212
6.36	Videoüberwachung durch Rechtsanwaltskanzlei	213
6.37	Allgemeine Anfragen zur Videoüberwachung	215
6.38	Videoüberwachungsverbesserungsgesetz – Verbesserung? – Anwendbarkeit?	218
6.39	Keine Meldepflicht bei Firmenüberwachung?.....	221
6.40	Baden und Entspannen unter Beobachtung – Videogaga 18.....	222
6.41	Videoüberwachung im Restaurant – bei nebulösen Angaben keine Beratung.....	225
6.42	Datenschutz: durchgesetzt! – Videogaga 19.....	227
6.43	Wenn der Datenschutz zweimal klingelt	227
6.44	Videoüberwachung versus Vandalen.....	229
6.45	Insolvenz schützt nicht vor Datenschutz – Videogaga 20	231
6.46	Hinweis auf Videoüberwachung, aber wo ist die Kamera?.....	232
6.47	Betreiber einer Videoüberwachung? – Ja Nein Vielleicht; Videogaga 21	233
6.48	Geschützte Fassaden.....	235
6.49	Die überwachte Datsche	238
6.50	Hausrecht – Video	239
6.51	Mein schöner Garten!	241
6.52	Video bleibt datenschutzrechtlich schwierig!	242
6.53	Alle Wege führen zum Kindergarten: Videogaga 22	244
6.54	Bewachter Parkplatz	246
6.55	Planung einer Videoüberwachung – der TLfDI hilft auch hier	248
6.56	Nette Familie	249
6.57	Kamerainstallation oder nicht, das ist hier die Frage	250
6.58	Ich glaub, ich steh im Wald	251
6.59	Problemzonen im Autohaus – Fortsetzung.....	254
6.60	Ob der Lkw richtig steht, sieht man, wenn die Kamera angeht – Videogaga 23	256
6.61	Streetview outsourced – davon wird’s nicht besser; Videogaga 24.....	258
6.62	Die (Un)zulässigkeit von Dashcams oder Die Leiden des (jungen) Hobbyfilmern	259

6.63	Nicht alle Wege führen zum Friedhof	264
6.64	Rundumüberwachung durch den Nachbarbetrieb? ..	265
6.65	Wertvoller Schrott im Fokus – Fortsetzung	268
6.66	Videoüberwachung als Auszugsgrund?	270
6.67	Videoüberwachungskamera auf der anderen Straßenseite	271
6.68	Apotheken-Video – Videogaga 25	273
6.69	Wenn der Thermenbesuch beobachtet wird – Videogaga 26	274
6.70	Wildtierkameras	276
6.71	Spielhalle: Videogaga 27	278
6.72	Fahrgäste im Visier – Videogaga 28	281
6.73	Kameras im Imbiss – Videogaga 29	285
6.74	Mieter unter Beobachtung – Videogaga 30	287
6.75	Videokameras als Türsteherersatz? – Videogaga 31	290
7	Beschäftigtendatenschutz	293
7.1	Videoüberwachung im Freizeitpark	293
7.2	Frau am Facebook-Pranger	295
7.3	(K)ein Kraftaufwand: Videoüberwachung im Fitnessstudio	297
7.4	Mit GPS immer ein Auge auf die Mitarbeiter?	298
7.5	Was ist vor der Inbetriebnahme einer Kamerainstallation zu beachten?	300
7.6	Datenschutz in der Altenhilfe: Wer hat wo- wann- wem geholfen?	303
7.7	Bewerbungsverfahren abgeschlossen – Bewerberdaten gelöscht?	304
7.8	Wenn der Chef weiß, dass der Mitarbeiter zur Konkurrenz will	306
7.9	Betriebsärztliche Untersuchungen: keine automatische Schweigepflichtentbindung im Arbeitsvertrag	308
7.10	Auskunftspflicht von Unternehmen	309
7.11	GPS für Arbeitgeber attraktiv – aber oft unzulässig	311
7.12	Lehrlinge im Fokus – kein Videogaga bei Nichterkenntbarkeit	312
7.13	Anfrage zum Passwortschutz von Arbeitsplatzrechnern	313
7.14	Veröffentlichen von Bildern behinderter Menschen	315

7.15	Beschäftigtendatenschutz – lückenlose Leistungs- und Verhaltenskontrolle unzulässig.....	316
7.16	Satte Rabatte contra Beschäftigtendatenschutz	317
7.17	Arbeitszeitüberwachung: nur datenschutzgerecht, wenn ... – Videogaga 32	319
7.18	Leistungsdruck durch GPS	321
7.19	Gab ein Arbeitsvermittler die Bewerbungsunterlagen seiner Mitarbeiterin ungefragt weiter?.....	322
7.20	Kündigung wegen Bewerbung in einem anderen Unternehmen?.....	324
7.21	Jobsuche und alle wissen es.....	325
7.22	Kontrolle in einem Logistik-Unternehmen.....	327
8	Werbung.....	330
8.1	Beschwerde über aufdringliche Telefonwerbung	330
8.2	Auch Werbe-E-Mails entgehen dem Datenschutz nicht	332
9	Auskunfteien	334
9.1	Verhindert die SCHUFA Dispositionskredit?	334
9.2	Überraschung: Ware nur nach Bonitätsabfrage	335
9.3	Schweigen eines Versandhandels	337
10	Gesundheit.....	340
10.1	Ansteckende Krankheiten sind Privatsphäre, oder nicht?	340
10.2	Antworten zum betriebsärztlichen Datenschutz	342
10.3	Der Apotheker als Ermittlungshelfer der Polizei? ...	345
10.4	Datenschutz bald verschreibungspflichtig?	347
10.5	Patientendaten unverschlüsselt im IT-Dschungel....	348
10.6	Einsicht in die Patientenakte – beim Therapeuten oder bei dessen Anwalt?	351
10.7	Fotoshooting in der Arztpraxis – wenn der Patient ungewollt zum Model wird.....	354
10.8	Fotoshooting in der Arztpraxis	355
10.9	Datenspeicherung in Apotheke: Kommerz versus Recht.....	357
10.10	Daten im Wartezimmer?.....	359
10.11	Datenschutz beim Zahnarzt: TLfDI bohrt nach	360
10.12	Auch Krankenhäuser von DS-GVO betroffen.....	362

10.13	Schreddern im Krankenhaus.....	364
10.14	Einwilligungserklärung bei Ärzten – So einfach geht das nicht!	366
10.15	Erwachsene familienversicherte Patienten sind mündig – eine Erhebung von Hauptversichertendaten entfällt damit!.....	368
10.16	Beratung durch den Amtsarzt verstößt nicht gegen den Datenschutz	369
10.17	Ist die Weitergabe der Personaldaten an die Heimaufsicht erlaubt?	371
10.18	Datenverarbeitung im Auftrag – ein Klinikum war gut vorbereitet.....	372
10.19	Bestellung von Arzneimitteln mit WhatsApp.....	375
10.20	Wearables und Gesundheits-Apps immer datenschutzkonform?	376
10.21	Beschwerde über ein Reinigungsunternehmen wegen nicht korrekt vernichteter Nachweisblätter.....	377
10.22	Urkundenverifikationsdienst Approbationsurkunden	378
11	Ordnungswidrigkeiten	381
11.1	Bußgelder nehmen stetig zu.....	381
12	Technischer und organisatorischer Datenschutz	384
12.1	Windows 10, Microsoft-Cloud Deutschland und Windows Office 365.....	384
12.2	Kritische Infrastruktur – Sektor Gesundheit	386
12.3	Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung.....	387
12.4	Datenschleudern – vom vernetzten Auto	389
12.5	Pflichten sozialer Netzwerke	393
12.6	Google-Analytics.....	395
12.7	Speicherung von IP-Adressen – Sicherheit oder Datenschutz?	396
12.8	eIDAS – was ist das?	399
12.9	EU- und nationale Cybersicherheit.....	400
12.10	Internationale Arbeitsgruppe zum Datenschutz in der Tele-kommunikation („Berlin Group“)	402
12.11	Wenn Kühlschränke eiskalt angreifen	403
12.12	Canvas-Fingerprinting	405

12.13	Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat.....	407
12.14	WannaCry.....	408
12.15	Zerstören Sie die Cayla-Puppe – wenn das Spielzeug mithört	410
13	Veranstaltungen.....	412
13.1	Profiling	412
13.2	Zusammenarbeit mit dem ERFA-Kreis Thüringen..	414
14	Vorträge – der TLfDI ist unterwegs!	416

Anlagen

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich

(Düsseldorfer Kreis am 13./14. September 2016)

Anlage 1	Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung.....	429
----------	--	-----

Entschließung der 91. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. April 2016 in Schwerin

Anlage 2	Wearables und Gesundheits-Apps –Sensible Gesundheitsdaten effektiv schützen!	430
----------	--	-----

Entschließung zwischen den Konferenzen 2017

Anlage 3	Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!	433
----------	---	-----

Pressemitteilungen 2016

Anlage 4	Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!....	435
----------	---	-----

Pressemitteilungen 2017

Anlage 5	Meldepflicht für (Wild-)Kameras bestätigt!	436
Anlage 6	Microsoft trifft TLfDI-Wirtschaft und Datenschutzaufsicht – geht das zusammen?.....	437
Anlage 7	Immelborn – AdActa	438

Kurzpapiere

Anlage 8	Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO	440
Anlage 9	Aufsichtsbefugnisse/Sanktionen	444
Anlage 10	Verarbeitung personenbezogener Daten für Werbung	448
Anlage 11	Datenübermittlung in Drittländer.....	452
Anlage 12	Datenschutz-Folgenabschätzung, Art. 35 DS-GVO	458
Anlage 13	Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO	467
Anlage 14	Markortprinzip: Regelungen für außereuropäische Unternehmen	471
Anlage 15	Maßnahmenplan „DS-GVO“ für Unternehmen.....	475
Anlage 16	Zertifizierung nach Art. 42 DS-GVO	480
Anlage 17	Informationspflichten bei Dritt- und Direkterhebung	484
Anlage 18	Recht auf Löschung / „Recht auf Vergessenwerden“	490

Abkürzungsverzeichnis.....	494
-----------------------------------	------------

Stichwortverzeichnis/ Index	498
--	------------

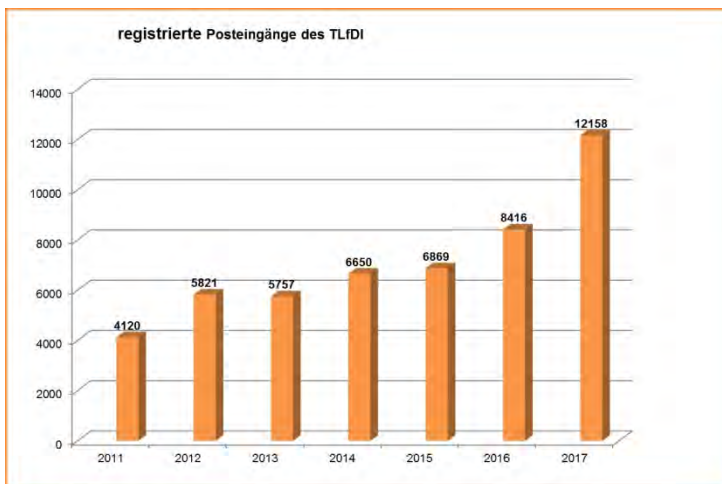
B Nicht-öffentlicher Bereich



Dr. Lutz Hasse

Vorwort

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist es offenbar gelungen, den Datenschutz im Freistaat Thüringen zu etablieren. Dies zeigt sich nicht nur am erneut signifikanten Umfang des Tätigkeitsberichts, sondern eben auch an der erfreulichen Statistik der Posteingänge.



Hier wird nicht nur optisch deutlich, dass die Nachfrage nach Datenschutz deutlich und stetig steigt, sondern hervorzuheben sind zudem zwei Aspekte: Von 2011 bis 2017 hat sich die Zahl der Posteingänge verdreifacht! Zudem macht der deutliche Anstieg im Jahr 2017 deutlich: Bürgerinnen und Bürger, aber auch Unternehmen, haben nachhaltig die Scheu vor dem TLfDI verloren. Zum anderen wirkt die Europäische Datenschutzgrundverordnung (EU-DS-GVO), die im Mai 2018 wirksam werden wird, ihre Schatten voraus. Deutlich spürbar ist in der Behörde des TLfDI der Anstieg der Anfragen von Bürgerinnen und Bürgern und Unternehmen zu dieser neuen Rechtsmaterie. Das alte Bundesdatenschutzgesetz wird zu dem genannten Zeitpunkt ausgedient haben; allerdings enthält die EU-DS-GVO sogenannte Öffnungsklauseln, die es den nationalen Gesetzgeber erlauben, im Rahmen der EU-DS-GVO-Vorgaben eigene Regelungen zu treffen. In einem neuen Bundesdatenschutzgesetz, das ebenfalls im Mai 2018 Wirkung entfalten wird, hat der Bundesgesetzgeber dies getan; das Werk kann nicht durchweg als geglückt angesehen werden, sodass der Fall eintreten kann, dass ein der EU-DS-GVO widersprechendes Bundesdatenschutzgesetz aufgrund des Anwendungsvorrangs des Europarechts nicht zur Umsetzung gelangt. Misslich für den deutschen Rechtsanwender ist zudem, dass künftig nicht mehr ein Blick in das neue Bundesdatenschutzgesetz oder die unmittelbar geltende EU-DS-GVO genügt, sondern ein

Zusammenlesen beider Gesetzesmaterien erforderlich ist, um den Willen der Gesetzgeber zu ermitteln. Das dürfte auch für spezialisierte Juristen kein leichtes Unterfangen werden – die Bürgerinnen und Bürger dürften hiermit überfordert sein. Der TLfDI ist hier natürlich die richtige Anlaufstelle, um auch komplexe Rechtsfragen zu beantworten.

Ein weites Feld tut sich auf bei der Digitalisierung von Fahrzeugen (Connected Cars), Arbeit 4.0, Industrie 4.0, Internet of Things (IoT) und Internet of Bodies (IoB). Die Bemerkung der Bundeskanzlerin Merkel, Daten seien der Rohstoff der Zukunft, hat aus Datenschutzsicht unheilvolle Aktivitäten ausgelöst und hier und da den Eindruck erweckt, man dürfe alles Menschenmögliche unternehmen, um Daten zu ökonomisieren. In den Hintergrund gerückt ist hierbei offenbar, dass die Daten-Kommerzialisierung nur im Rahmen des rechtlich Möglichen erfolgen darf. Hier ist sorgsam darauf zu achten, dass das Grundrecht der informationellen Selbstbestimmung nicht unter die Räder gerät. Technische Entwicklungen und deren Anwendungen setzen Fakten, die datenschutzrechtlich nicht abgeklopft sind. Das ist nicht nur eine Meinung des TLfDI und anderer Landesbeauftragter, sondern auch Meinung der Akteure selbst. Der Kontakt zwischen TLfDI und Thüringer Wirtschafts-Digitalministerium steht, um in Thüringen datenschutzrechtskonforme Wege zu beschreiten, was durchaus möglich ist, ohne Wirtschaftsinteressen übermäßig zu belasten. Dessen ungeachtet hat der TLfDI die Kontakte zu den Industrie- und Handelskammern sowie zur Handwerkskammer intensiviert, was sich nicht nur in der gemeinsamen Erstellung von Flyern und Informationsblättern niederschlägt, sondern von zunehmender Bedeutung dafür ist, dass über die genannten Organisationen die erwähnten Neuerungen im Datenschutzrecht an die Wirtschaftsakteure auch künftig in verstärktem Maße gesteuert werden können. Der TLfDI sieht seine Aufgabe auch künftig darin, die Verarbeitung personenbezogener Daten im Vorfeld mit den Unternehmen zu erörtern, um allen Beteiligten Verwaltungs- und Bußgeldverfahren zu ersparen.

Auch an dieser Stelle möchte ich es nicht versäumen meinen Mitarbeiterinnen und Mitarbeitern herzlich für ihr Engagement und ihre Motivation, für den Datenschutz zu streiten, zu danken! Ohne ein solches schlagkräftiges Team stünde der Datenschutz im Freistaat Thüringen im Vergleich mit den anderen Bundesländern nicht auf einem der vorderen Plätze.

Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: <https://www.tlfdi.de/tlfdi/>). Dadurch kann auf Gerä-



ten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden Software der Link durch das Gerät wieder decodiert und „Abschreibfehler“ können vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers Marty Mouse in der Version 1.0 empfohlen werden, da hier Open-Source-Software genutzt wird

und die App nur minimale Funktionen besitzt. Für iOS ist dem TLFDI keine datenschutzgerechte App bekannt.



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

1 Schwerpunkte im Berichtszeitraum

Leider ungebrochen ist der Trend in Thüringen, Videotechnik im privaten Bereich, aber auch in Unternehmen einzusetzen. Verstärkt wird dieser Trend durch den Einsatz von sogenannten Dashcams in Fahrzeugen, durch Kameras in Fahrrad- und Motorradhelmen und durch Drohnen mit ausgefeilter Videotechnik. Dass Videokameras einer Meldepflicht gemäß § 4d Bundesdatenschutzgesetz unterliegen – so jüngst das OVG Saarlouis –, scheint noch nicht bei jedem Videobetreiber angekommen zu sein, trotz mehrfacher Hinweise des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) dazu. Das Versäumen der genannten Meldepflicht stellt eine Ordnungswidrigkeit dar. Die Rechtsprechung insbesondere zu Dashcams ist noch uneinheitlich, aus Sicht des TLfDI zeichnet sich indes inzwischen die Tendenz ab, Dashcams grundsätzlich für datenschutzrechtswidrig zu erklären, wenn fortlaufend personenbezogene Daten Dritter erhoben und weiterverarbeitet werden. Zahlreiche Verwaltungsgerichts- und Bußgeldverfahren nicht nur in Videoangelegenheiten hat der TLfDI neuerdings zu bearbeiten, so dass der Gedanke naheliegt, in der Behörde ein eigenes Justizariat einzurichten.

Der TLfDI bleibt auch von Wahlkämpfen nicht verschont und war bzw. ist gehalten, den datenschutzrechtskonformen Einsatz von Wahlkampf-Apps zu überprüfen. Mehrere Landesdatenschutzbeauf-

trage sind in diesen Prozess involviert, und man wird am Ende dieses Prozesses sehen, ob wir auch in diesem sensiblen Bereich unter Auswertung von Big Data auf dem Weg in amerikanische Verhältnisse sind, wo der gläserne Bürger längst die neue Spezies ist. „No Privacy“ mag für viele schick sein, steht indes im Widerspruch zum Grundrecht der informationellen Selbstbestimmung, dessen Bedeutung den Bürgerinnen und Bürgern offenbar immer deutlicher wird.

Die Landesdatenschutzbeauftragten stehen mit der Versicherungswirtschaft in intensiven Verhandlungen, um auch vor dem Hintergrund der künftigen Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) Datenübermittlungen in das außereuropäische Ausland abzustimmen. Die Digitalisierung macht auch im Beschäftigtendatenschutz nicht halt. Der Einsatz von Videotechnik, GPS und anderen Leistungskontrollmechanismen beschäftigt den TLfDI in zunehmendem Maße. Nicht selten wird eine verdeckte Leistungskontrolle der Mitarbeiterinnen und Mitarbeiter kaschiert mit dem Scheinargument, die eingesetzte Technik Sorge für die Sicherheit des Mitarbeiters bzw. der Mitarbeiterin. Der TLfDI konnte im Berichtszeitraum Auswüchsen in dieser Richtung wirksam entgegenwirken.

Auch im Gesundheitsbereich hält die Digitalisierung an. Die Krankenhausinformationssysteme werden leistungsfähiger, können damit den Datenschutz immer besser abbilden, sind allerdings auch in der Lage, immer größere Datenmengen zu bestimmten Zwecken zu verarbeiten. Datenflüsse zwischen verschiedenen Einrichtungen des Gesundheitswesens bedürfen klarer Regelungen bzw. der Einwilligung eines informierten Patienten. Beides lässt bisweilen zu wünschen übrig, allerdings ist es dem TLfDI in Kooperation mit der Landeskrankenhausesellschaft Thüringen e. V. gelungen, datenschutzrechtskonforme Lösungen zu finden, die auch in der Praxis Akzeptanz finden.

Die große Dynamik bei der Kommerzialisierung von Daten, die von Big Data, Datamining und dem intransparenten Einsatz von Algorithmen befeuert wird, sollte nicht nur die Landesdatenschutzbeauftragten zum Nachdenken zwingen. In fortschreitendem Tempo setzen Entwicklungen ein, denen der Gesetzgeber nicht mehr Herr zu werden scheint. Das Grundrecht der informationellen Selbstbestimmung – so das Bundesverfassungsgericht – wurzelt in der Menschenwürde. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt (Artikel 1 Abs. 1 Satz 2 Grundgesetz). Die augenfälligen Bedrohungen des Grundrechts der informationellen Selbst-

bestimmung, gerade auch im Unternehmensbereich, könnten und sollten daher durchaus deutlichere staatliche Aktivitäten zum Schutz dieses Grundrechts auslösen.



Datenschutz (Anwalt, Datenschutzbeauftragter) - © fotodo / fotolia.com

2 Der betriebliche Datenschutzbeauftragte

2.1 Europäische Datenschutz-Grundverordnung: Unternehmen fragen – TLfDI informiert

Im Berichtszeitraum wandte sich ein Mitarbeiter eines Unternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und erkundigte sich nach den Voraussetzungen der Bestellpflicht eines behördlichen Datenschutzbeauftragten (bDSB) nach der europäischen Datenschutz-Grundverordnung (DS-GVO). Er wollte wissen, inwieweit Datenschutzbeauftragte in Unternehmen bzw. externe Datenschutzbeauftragte unter Geltung der Datenschutz-Grundverordnung noch benötigt werden bzw. ob in der Datenschutz-Grundverordnung das Bestellen eines Datenschutzbeauftragten (intern oder extern) geregelt ist.

Nach derzeitigem Stand stellt sich die Rechtslage folgendermaßen dar:

In Artikel 37 Absatz 1 DS-GVO ist klar definiert, wann Verantwortliche und Auftragsdatenverarbeiter einen internen Datenschutzbeauftragten zu benennen haben. Und zwar in drei Fällen. Zunächst haben

öffentliche Stellen, sofern sie personenbezogene Daten verarbeiten, stets einen Datenschutzbeauftragten zu bestellen. Ausgenommen sind Gerichte im Rahmen rechtssprechender Tätigkeit. Nicht-öffentliche Stellen, also natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, haben einen Datenschutzbeauftragten zu bestellen, wenn deren Kerntätigkeit oder die Kerntätigkeit desjenigen, der Daten im Auftrag verarbeitet (Auftragsdatenverarbeitung), in einer Datenverarbeitung besteht,

- die aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erfordert oder
- die eine umfangreiche Verarbeitung von Daten, die nach Artikel 9 oder 10 DS-GVO besonders schutzwürdig sind, umfasst.

Der Erwägungsgrund 97 zum Artikel 37 DS-GVO stellt klar, dass das „Kerngeschäft“ die Hauptaktivität des Unternehmens meint. Bloße Nebentätigkeiten sollen nicht darunter fallen.

Verantwortliche oder Auftragsdatenverarbeiter können selbstverständlich auch freiwillig einen Datenschutzbeauftragten bestellen. Artikel 37 Abs. 4 DS-GVO enthält aber auch eine Öffnungsklausel, mit der den Mitgliedsstaaten die Möglichkeit eingeräumt wird, im nationalen Recht für weitere Fälle die Bestellung eines Datenschutzbeauftragten vorschreiben zu können.

Hiervon hat der Bundesgesetzgeber Gebrauch gemacht und in § 38 des neuen Bundesdatenschutzgesetzes (BDSG) eine Regelung geschaffen, die über die o. g. Bestellpflichten hinausgeht. Hier heißt es im Absatz 1, ergänzend zum Artikel 37 Absatz 1 Buchstabe b und c DS-GVO, die Verantwortlichen und der Auftragsdatenverarbeiter haben einen Datenschutzbeauftragten zu benennen, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Des Weiteren haben sie einen Datenschutzbeauftragten zu benennen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung nach Artikel 35 DS-GVO unterliegen. Auch wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Marktforschung verarbeitet werden, haben die Verantwortlichen unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

Artikel 37 Abs. 1 DS-GVO regelt die Benennung eines Datenschutzbeauftragten. Zu beachten sind die in Absatz 4 benannten Öffnungsklauseln. Zum einen können Datenschutzbeauftragte freiwillig bestellt werden und zum anderen haben die Mitgliedstaaten die Möglichkeit, im nationalen Recht weitere Fälle der Bestellung eines Datenschutzbeauftragten zu regeln. § 38 BDSG besagt, dass – ergänzend zum Artikel 37 Absatz 1 Buchstabe b und c DS-GVO – die Verantwortlichen und der Auftragsverarbeiter einen Datenschutzbeauftragten zu benennen haben, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Des Weiteren haben sie einen Datenschutzbeauftragten zu benennen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung nach Artikel 35 DS-GVO unterliegen. Auch wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Marktforschung verarbeitet werden, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

2.2 Darf ein IT-Mitarbeiter gleichzeitig betrieblicher Datenschutzbeauftragter sein?

Im Berichtszeitraum bat ein IT-Mitarbeiter eines Unternehmens den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Mitteilung, ob er im Hinblick auf die Qualifikationsvoraussetzungen für die Position des betrieblichen Datenschutzbeauftragten (bDSB) seiner Firma in Betracht käme. Die Geschäftsführung seiner Firma würde dieser Tätigkeit zustimmen, sofern der Mitarbeiter eine entsprechende Fortbildung absolviert und keine Bedenken im Hinblick auf Interessenkonflikte bestünden.

Der IT-Mitarbeiter war bei einer Ingenieursgesellschaft angestellt, die zu einer Firmengruppe gehörte und vollständig in deren Netzwerk integriert war. Alle relevanten IT-Entscheidungen wurden vom Hauptsitz getroffen und von den Standorten umgesetzt. Der Mitarbeiter war an „seinem“ Standort IT-Verantwortlicher und nur der dortigen Geschäftsführung als Mitarbeiter unterstellt. Ein Weisungsrecht im Rahmen seines Arbeitsverhältnisses bestand nur seitens der Geschäftsführung an „seinem“ Standort und nicht von Seiten des Hauptsitzes.

Nach Angaben des IT-Mitarbeiters wurden alle relevanten IT-Entscheidungen vom Hauptsitz der Firmengruppe vorgegeben, die lokalen Administratoren erhielten die Berechtigungen von dort und mussten die IT-Richtlinien an den jeweiligen Standorten umsetzen. Ebenfalls wurden die User-Protokolle sowie die persönlichen Daten der User über Gruppenrichtlinien zentral vom Hauptsitz administriert. Die jeweiligen Standortadministratoren haben keinen eigenen Zugriff; die Rechtevergabe erfolgte vom Hauptsitz aus, lediglich die Vergabe der Zugriffsrechte auf Projektdaten erfolgte eigenständig an den Standorten.

Der TLfDI hatte gegen die Bestellung des IT-Mitarbeiters zum betrieblichen Datenschutzbeauftragten keine Bedenken. Er wies jedoch darauf hin, dass das Unternehmen darauf achten müsse, dass beide Aufgabenbereiche des Mitarbeiters – als bDSB und als nachgeordneter IT-Administrator in der Ingenieursgesellschaft – klar voneinander getrennt sind. Die klare Trennung dieser Positionen voneinander muss gewährleistet und dokumentiert werden; hierfür trägt das Unternehmen die Verantwortung ebenso wie für die ordnungsgemäße Bestellung des bDSB.

Seine Auffassung begründete der TLfDI folgendermaßen: Der Gesetzgeber hat in § 4f Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) zwei Qualifikationsmerkmale für einen bDSB festgelegt: Fachkunde und Zuverlässigkeit. Hieraus lässt sich jedoch kein festes Anforderungsprofil für diese Funktion bilden. Eine ausreichende Fachkunde kann nur dann angenommen werden, wenn die Person sowohl über entsprechende rechtliche als auch organisatorische und technische Kenntnisse verfügt. Um die Anforderungen und Ziele von datenschutzrelevanten rechtlichen Regelungen zu erkennen und deren Konsequenzen für die verantwortliche Stelle bewerten zu können, sind ausreichende rechtliche Kenntnisse zwingend erforderlich. Allgemeine überblicksartige Kenntnisse wären hierfür nicht ausreichend.

Dies liegt darin begründet, dass das Bundesdatenschutzgesetz (BDSG) durch eine ungewöhnlich hohe Zahl an Generalklauseln gekennzeichnet ist. Daher muss der bDSB in der Lage sein, eine datenschutzkonforme Interpretation dieser Klauseln auch dann zu vertreten, wenn die vom Gesetzgeber geschaffenen Normen nur auf den ersten Blick keine klare Lösung aufzeigen, bei näherer Betrachtung jedoch Interpretationsspielraum zulassen.

Ein zu ernennender bDSB muss darüber hinaus sehr zuverlässig sein, sowohl in objektiver wie in subjektiver Hinsicht. Dabei beziehen sich die subjektiven Aspekte auf persönliche Eigenschaften und die objektiven Faktoren auf mögliche Interessenkollisionen. Diesbezüglich ist darauf zu achten, dass kein Interessenkonflikt zwischen der arbeitsstellenbezogenen Tätigkeit als IT-Mitarbeiter und den inhaltlichen Aufgaben des bDSB im Unternehmen besteht. Die subjektiven Aspekte hingegen können vom TLfDI nicht überprüft werden. Dabei handelt es sich um in der Person liegende Gründe, die zu einer Unzuverlässigkeit führen, wie beispielsweise dem aus der Vergangenheit bekannten sorglosen Umgang mit personenbezogenen Daten.

Grundsätzlich ist davon auszugehen, dass ein IT-Leiter und ein bDSB widerstrebende Interessen haben, sodass ein IT-Mitarbeiter nicht als bDSB bestellt werden sollte. Dies legt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Website dar: *„Interessenkonflikte können insbesondere dann auftreten, wenn der bDSB gleichzeitig Aufgaben in den Bereichen Personal, Infor-*



mationstechnik oder in Organisationseinheiten mit besonders umfangreicher oder sensibler Verarbeitung von personenbezogenen Daten wahrnimmt oder Geheimschutzbeauftragter ist.“

(vgl. <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/m/m02/m02502.html>). Jedoch gibt das BSI auf seiner Website unter M 2.502, Regelung der Verantwortlichkeiten im Bereich Datenschutz, im Abschnitt „Bestellung eines Datenschutzbeauftragten“ auch nähere Hinweise, wie entsprechende Interessenkonflikte gelöst werden können: *„Möglich ist (...) die Zusammenlegung der Funktionen des bDSB mit denen des IT-Sicherheitsbeauftragten. Ist der IT-Sicherheitsbeauftragte organisatorisch unabhängig von der für die IT verantwortlichen Organisationseinheit eingerichtet, ist die Zusammenfassung in einer Hand empfehlenswert.“* (vgl. a.a.O.)

Aufgrund der vom IT-Mitarbeiter beschriebenen Firmenorganisation und seines Arbeitsbereiches bestand aus Sicht des TLfDI ein Abhängigkeitsverhältnis des Mitarbeiters als Teil des regionalen IT-Bereichs zum IT-Leiter der Firmengruppe am Hauptsitz. Daher sollte

ergänzend dokumentiert werden, wie die Handlungsfähigkeit als bDSB gegeben ist, wenn IT-Richtlinien des Hauptstandorts gegen die Interessen des bDSB verstoßen. Weiterhin ergibt sich der notwendige Ergänzungsbedarf aufgrund der Tatsache, dass die Ingenieurgesellschaft eigenständig arbeitet und IT-bezogen lediglich Richtlinien und Vorgaben der Firmengruppe in Bezug auf IT-Strategie, Sicherheitseinstellungen, User-Rechte umsetzt.

Da Dienstleistungen gegenseitig in Rechnung gestellt werden, war nach Ansicht des TLfDI auch vertragsbezogen davon auszugehen, dass eine formale Unabhängigkeit zwischen der Ingenieurgesellschaft und der Firmengruppe bestand. Die Ausführungen des IT-Mitarbeiters zu seiner Arbeit als Softwareentwickler ließen zweifelnsfrei erkennen, dass in Bezug auf diese Tätigkeit kein Widerspruch zu einer möglichen Bestellung zum bDSG vorlag.

Der TLfDI empfahl dem IT-Mitarbeiter abschließend, vor der Berufung zum bDSB für das Erlangen der entsprechenden Fachkunde eine Schulung zu belegen, sofern die nötigen Kenntnisse noch nicht vorhanden sein sollten, da mangelnde Sachkunde dazu führt, dass die Bestellung unwirksam ist.

Klarstellend wird darauf hingewiesen, dass ein IT-Mitarbeiter nichts mit der Position IT-Sicherheitsbeauftragter zu tun hat. Bei Letzterem besteht wegen der Kollision von Aufgaben und Beratungsverpflichtungen immer ein Interessenskonflikt, mit der Folge der Unzulässigkeit der Bestellung als bDSB, s. a. Beitrag 2.3.

In Einzelfällen kann ein Mitarbeiter der IT-Abteilung auch bDSB des Unternehmens sein. Es muss jedoch sorgfältig sichergestellt werden, dass keine Interessenskollisionen bestehen. Stellt der TLfDI bei einer späteren Prüfung solche Kollisionen fest, ist die Bestellung ab Bestehen dieser Kollisionen als unwirksam zu bewerten. Dies führt, wenn das Unternehmen zur Bestellung eines bDSB verpflichtet ist, in der Regel auch zu einem Ordnungswidrigkeitenverfahren.

2.3 Darf ein IT-Sicherheitsbeauftragter gleichzeitig Datenschutzbeauftragter des Unternehmens sein?

Im Berichtszeitraum richtete der Mitarbeiter eines Unternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit TLfDI die Anfrage, ob die Funktionen des IT-Sicherheitsbeauftragten und die des internen betrieblichen Daten-

schutzbeauftragter (bDSB) von dem gleichen Mitarbeiter ausgeübt werden können oder ob dies zu Interessenkonflikten führe.

Nach Prüfung des Sachverhalts gelangte der TLfDI zu der Ansicht, dass in dieser Konstellation Interessenkonflikte drohen und daher eine Bestellung des besagten Mitarbeiters zum bDSB nicht wirksam wäre. Nach Auffassung des TLfDI ist nicht pauschal davon auszugehen, dass ein IT-Sicherheitsbeauftragter nicht zuverlässig im Sinne des § 4f Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) ist. Das Bundesdatenschutz (BDSG) hat in § 4f Abs. 2 Satz 1 BDSG die Bestellung des Beauftragten an zwei Qualifikationsmerkmale geknüpft: Fachkunde und Zuverlässigkeit. Bei der Zuverlässigkeit sind subjektive genauso wie objektive Faktoren zu bedenken. Die subjektiven Aspekte beziehen sich auf persönliche Eigenschaften, die objektiven auf mögliche Interessenkollisionen. Eine Bestellung zum bDSB kann daher nur erfolgen, wenn neben den subjektiven Voraussetzungen keine Interessenkollisionen zwischen den unterschiedlichen Arbeitsfunktionen vorliegen.

Die Kenntnisse und Erfahrungen des IT-Sicherheitsbeauftragten im Bereich der Datensicherheit sprechen zwar für eine Bestellung zum bDSB, jedoch wird die Zuverlässigkeit durch mögliche Interessenkonflikte infrage gestellt. Der IT-Sicherheitsbeauftragte eines Unternehmens ist gemäß seiner Position und Funktion berechtigt, Grundsätze festzulegen, nach denen sich das Unternehmen als verantwortliche Stelle zur Bestellung des bDSB richten muss. Insofern trägt er hierfür auch die Verantwortung. Darüber hinaus besitzt er eine unabhängige und organisatorisch herausgehobene Stellung. Er ist in dieser Rolle der Unternehmensführung direkt unterstellt und berichtet an diese. Sollte er eigenverantwortlich für die Umsetzung der IT-Sicherheitsstandards zuständig und somit direkt dem Leiter der EDV unterstellt sein, würde dies im Widerspruch zur unabhängigen Stellung eines Datenschutzbeauftragten stehen. Die Zuverlässigkeit im Sinne des § 4f Abs. 2 Satz 1 BDSG könnte daher nicht mehr sichergestellt werden.

Darüber hinaus muss bei der Abgrenzung, wann die erforderliche Zuverlässigkeit aufgrund bestehender Interessenkollision nicht mehr gegeben ist, der Einsatzbereich der betroffenen Person als Arbeitnehmer besonders berücksichtigt werden. Dies betrifft insbesondere die Frage, ob die Person auch damit betraut ist, die datenschutzkonforme Verarbeitung personenbezogener Daten (Einzelangaben über persönliche und wirtschaftliche Verhältnisse der Beschäftigten ge-

mäß § 3 Abs. 1 BDSG), zu sichern. In einer solchen Konstellation würde die parallele Wahrnehmung der gesetzlichen Aufgaben als bDSB auf eine Kontrolle der eigenen Arbeit hinauslaufen (vgl. BDSG/Simitis, 8. Aufl., § 4f Rn. 100 ff.). Denn im Rahmen seiner Tätigkeit muss der bDSB auf die Einhaltung aller datenschutzrechtlichen Bestimmungen im Bereich personenbezogener Daten hinwirken (§ 4f Abs. 1 Satz 1 BDSG).

Grundsätzlich sind daher beide Funktionen nach Auffassung des TLfDI nicht miteinander vereinbar.

Die Funktionen des IT-Sicherheitsbeauftragten und die des betriebsinternen Datenschutzbeauftragten (bDSB) eines Unternehmens durch den gleichen Mitarbeiter kann zu Interessenkollisionen führen. Dies ist insbesondere der Fall, wenn der regelmäßige Arbeitsbereich des Mitarbeiters sich auch auf die Sicherung der datenschutzkonformen Verarbeitung personenbezogener Daten bezieht. In diesem Falle würde die parallele Wahrnehmung der Aufgaben des bDSB auf eine Kontrolle der eigenen Arbeit hinauslaufen. Beide Funktionen sind daher grundsätzlich nicht miteinander vereinbar.

2.4 Zu viele auf einmal: Bestellung einer Rechtsanwalts-Partnerschaft zum Datenschutzbeauftragten

Im Berichtszeitraum wandte sich eine Rechtsanwalts-Partnergesellschaft mit einem Beratungersuchen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Kern der Beratungsanfrage war, ob der TLfDI es für zulässig erachtet, dass sich eine Partnerschaftsgesellschaft selbst zum betrieblichen Datenschutzbeauftragten bestellen lässt.

Die Rechtsanwalts-Partnerschaftsgesellschaft vertritt dabei die Auffassung, dass sie als Partnerschaft natürlicher Personen als externer Datenschutzbeauftragter auftreten kann. Sie sei keine juristische Person und verfüge über Fachkunde und Zuverlässigkeit, wie es vom Bundesdatenschutzgesetz (BDSG) gefordert wird. Sie stelle eine Bündelung von Expertenwissen bei wachsendem Bedarf an Professionalisierung und Spezialisierung des Datenschutzbeauftragten dar und gewährleiste darüber hinaus im Gegensatz zu einzelnen juristischen Personen höhere Kontinuität und Verfügbarkeit in der Beratung von Mandanten.

Grundsätzlich ist es nach dem BDSG möglich, dass nicht-öffentliche Stellen statt eines internen einen externen Datenschutzbeauftragten bestellen. Problematisch bei der Bestellung einer Rechtsanwalts-Partnersgesellschaft ist jedoch, dass die Funktion des Datenschutzbeauftragten durch eine unbestimmte Personengruppe mit gegebenenfalls wechselndem Personenbestand wahrgenommen würde.

Das BDSG regelt hierzu in § 4f Abs. 2 Satz 3, 1. HS Folgendes:

[...] Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; [...]

Zunächst ist dem Gesetzeswortlaut zu entnehmen, dass es sich beim externen Beauftragten um eine Person handeln muss. Dem deutschen Recht sind nur zwei Arten von Personen bekannt, die natürliche wie auch die juristische Person.

Dabei sind natürliche Personen alle Menschen. Juristische Personen hingegen sind eine Erfindung des Gesetzgebers. Sie existieren nur auf dem Papier und werden, um handlungsfähig zu sein, von natürlichen Personen vertreten. Gängigster Vertreter einer juristischen Person ist beispielsweise die GmbH.

Bei einer Partnerschaftsgesellschaft handelt es sich jedoch um eine Personengesellschaft und damit um einen Zusammenschluss aus mehreren natürlichen und/oder juristischen Personen. Eine Personengesellschaft ist daher bereits nach dem Wortlaut des Gesetzes ausgeschlossen.

Dies lässt sich ebenfalls historisch und europarechtlich untermauern. Weder das BDSG 77 noch das BDSG 90 (in beiden Fällen handelt es sich um alte Versionen des Bundesdatenschutzgesetzes) kannten den externen Datenschutzbeauftragten. Es war lediglich vom Datenschutzbeauftragten als Angestelltem innerhalb der verantwortlichen Stelle die Rede, also ausschließlich von einer natürlichen Person.

§ 4f Abs. 2 Satz 3 BDSG wurde erst durch Umsetzung der Datenschutzrichtlinie in das BDSG aufgenommen. Im Erwägungsgrund 49 zu dieser Richtlinie heißt es:

„Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können“.

Dem kann entnommen werden, dass auch der europäische Gesetzgeber ausschließlich natürliche Personen als interne wie auch externe betriebliche Datenschutzbeauftragte im Sinn hatte, als die entsprechende Richtlinie verfasst wurde.

Der TLfDI hat mitgeteilt, dass er dieser Auffassung nicht folge und die Bestellung einer Gesellschaft als betrieblicher Datenschutzbeauftragter nicht für zulässig erachtet.

Wenn Sie einen betrieblichen Datenschutzbeauftragten bestellen, muss es sich dabei um eine natürliche Person handeln. Andernfalls – etwa im Falle der Bestellung einer Personalgesellschaft – ist eine eventuelle Bestellung unwirksam. Mögliche Folge ist dann ein Bußgeldverfahren.

2.5 Bestellung eines Datenschutzbeauftragten

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) haben im Berichtszeitraum immer wieder Anfragen zur Bestellpflicht, zu den Aufgaben und der Stellung des betrieblichen Datenschutzbeauftragten (bDSB) im Unternehmen erreicht.

Der bDSB ist von nicht-öffentlichen Stellen, also von Unternehmen, immer dann notwendigerweise zu bestellen, wenn die Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen mehr als neun beträgt, § 4f Abs. 1 Satz 4 BDSG. Bei einer nicht-automatisierten Verarbeitung personenbezogener Daten ist ein Beauftragter immer dann zu bestellen, wenn mindestens zwanzig Personen dabei beschäftigt werden, § 4f Abs. 1 Satz 3 BDSG.

In Bezug auf die „Stelle“, die den Datenschutzbeauftragten bestellen muss, handelt es sich um die konkret betroffene juristische Person, Personengesellschaft oder Einzelperson. Gleichgültig ist, wie das Unternehmen organisatorisch im Einzelnen ausgestaltet ist und ob es aus einem oder mehreren Betrieben besteht. Für die Bewertung, wer „Stelle“ im Sinne des § 4f ist, zählt als Anknüpfungspunkt nur die jeweils rechtliche Einheit. Soweit ein Unternehmen also in mehrere rechtlich selbstständige Einheiten unterteilt ist, hat jede von ihnen einen eigenen bDSB zu bestellen.

Es kann sowohl ein interner Datenschutzbeauftragter als auch ein externer Datenschutzbeauftragter ernannt werden. Der interne Beauftragte übt seine Kontrollfunktion immer nur im Rahmen einer bestimmten verantwortlichen Stelle aus, bei der er selbst auch tätig ist. Der externe Beauftragte übt regelmäßig für mehrere oder eine Vielzahl von verantwortlichen Stellen die Kontrolle aus. Er ist selbst nicht in dem Unternehmen beschäftigt, sondern ist im Rahmen seiner

selbstständigen Tätigkeit für mehrere Unternehmen zuständig. Interne sowie externe Beauftragte unterliegen dabei jedoch den gleichen rechtlichen Anforderungen, vgl. Simitis, BDSG-Kommentar, § 4f, Rn. 46f.

Bei der Ernennung eines Beauftragten sind die Formerfordernisse des § 4f Abs. 1 Satz 2 BDSG zu beachten. Danach muss der Beauftragte spätestens einen Monat nach Beginn der Verarbeitung bei der verantwortlichen Stelle bestellt sein. Diese Bestellung hat schriftlich zu erfolgen, § 4 Abs. 1 Satz 1 BDSG. Das Erfordernis der Schriftlichkeit verlangt daher eine von beiden Parteien unterschriebene Urkunde. Die Schriftform ist zudem konstitutiv, d. h., fehlt es an einer solchen, ist die Verpflichtung zur Bestellung eines Beauftragten als nicht erfüllt anzusehen. Diese Verfehlung ist im Rahmen des BDSG auch mit einem Bußgeld bewehrt, § 43 Abs. 1 Nr. 2 BDSG.

Die Bestellung des Beauftragten ist weiterhin an zwei entscheidende Qualifikationsmerkmale geknüpft: Fachkunde und Zuverlässigkeit.

Die geforderte Fachkunde nach § 4f Abs. 2 Satz 1 BDSG beinhaltet Kenntnisse in rechtlicher, organisatorischer und technischer Hinsicht. Der Beauftragte muss über ausreichende rechtliche Kenntnisse verfügen, um den Hintergrund, Anforderungen und Ziel der datenschutzrelevanten rechtlichen Regelungen erkennen zu können und damit auch Rückschlüsse auf die möglichen Konsequenzen für die verantwortliche Stelle ziehen zu können. Allein summarische Kenntnisse sind an dieser Stelle nicht ausreichend.

Weiterhin sind organisatorische Kenntnisse notwendig, um Entscheidungsabläufe und Strukturen nachvollziehen und die ggf. notwendigen Korrekturen zur Erhaltung der datenschutzrechtlichen Konformität vornehmen zu können.

Schlussendlich muss der Beauftragte auch über technische Kenntnisse verfügen, da diese zu den Grundvoraussetzungen der Kontrollkompetenz eines jeden Beauftragten zählen.

Die geforderte Zuverlässigkeit des Beauftragten ist sowohl in subjektiver als auch in objektiver Hinsicht zu bewerten. Der Beauftragte sollte sich also in seinem bisherigen Verhalten hinsichtlich etwaiger datenschutzrechtlicher Verstöße unauffällig gezeigt haben.

In objektiver Hinsicht setzt eine verlässliche Kontrolle eine klare Trennung zwischen der verantwortlichen Stelle und dem Beauftragten voraus. Durch diese Trennung werden Interessenkonflikte vermieden. Diese entstehen immer dann, wenn der Beauftragte im Rahmen seiner Tätigkeit Entscheidungen zu treffen hat, die auch

datenschutzrechtliche Belange berühren. Der Interessenkonflikt ist am deutlichsten bei Firmeninhabern, Geschäftsführern, Vorständen oder sonstigen mit der Leitung der verantwortlichen Stelle betrauten Personen. Durch ihre Funktion und Position sind sie berechtigt, Grundsätze festzulegen, nach denen sich die Stelle bei ihrer Tätigkeit richten muss. Im Fokus stehen daher die Ziele und Interessen der verantwortlichen Stelle. Der Datenschutz würde hinter diesen an zweiter Stelle stehen und die Gefahr besteht, dass er aus der Sicht der Erwartungen der verantwortlichen Stelle interpretiert wird, was eine massive Interessenkollision darstellt. Diese Interessenkollision steht auch bei leitenden Angestellten wie Leitern der EDV-Abteilung, Marketingleitern, Personalleitern, Leitern der Rechtsabteilung, Leitern der Revisionsabteilung, Vertriebs- und Betriebsleitern im Raum, da diese sich im Rahmen ihrer Tätigkeit mit der Verarbeitung von personenbezogenen Daten beschäftigen und daher ebenfalls Situationen ausgesetzt sind, in denen sie aufgrund von unternehmensbezogenen Entscheidungen, die sie zu treffen haben, den Datenschutz dahingehend auslegen und dieser dadurch nicht immer die notwendige Berücksichtigung und Aufmerksamkeit findet.

Organisatorisch ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und ausschließlich dieser rechenschaftspflichtig. Der Beauftragte kann sich jederzeit an die Leitung der verantwortlichen Stelle wenden und auf notwendige Maßnahmen und festgestellte Verstöße aufmerksam machen. Er ist weisungsfrei, § 4f Abs. 3 Satz 2 BDSG, in der Wahrnehmung seiner gesetzlichen Aufgaben. Die verantwortliche Stelle hat ihn bei der Erfüllung seiner Aufgaben zu unterstützen und mit der notwendigen materiellen und personellen Ausstattung zu versorgen.

Die Bestellung des Beauftragten endet mit dem Ablauf der vereinbarten Bestellfrist oder, wenn eine solche nicht vereinbart wird mit der Amtsniederlegung durch den bDSB selbst oder mit dem Widerruf aus wichtigem Grund durch die verantwortliche Stelle, § 4 Abs. 3 Satz 4 BDSG. Der Widerruf kann bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde erfolgen.

Schlussendlich hat jeder Betroffene das Recht, den Beauftragten anzurufen, das heißt, sich mit seinem Anliegen an ihn zu wenden, § 4f Abs. 5 Satz 2 BDSG. Das Gesetz räumt damit die Möglichkeit ein, dass sich die Betroffenen Klarheit über den Umgang mit ihren

Daten verschaffen und damit ihre Rechte im Datenschutz besser wahren können.

Der Beauftragte für den Datenschutz wirkt auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin. Er überwacht die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen mit deren Hilfe personenbezogene Daten verarbeitet werden sollen. Er hat insbesondere auch die Personen die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, über die datenschutzrelevanten Vorschriften zu informieren.

Der betriebliche Datenschutzbeauftragte ist das Bindeglied zwischen den Interessen der verantwortlichen Stelle auf der einen Seite und den Rechten der Betroffenen auf der anderen Seite. Um einen verantwortungsbewussten Ausgleich im Rahmen der gesetzlichen Bestimmungen zwischen diesen beiden Positionen herzustellen muss der Beauftragte die nötigen Fachkenntnisse und die notwendige Zuverlässigkeit für diese Tätigkeit mitzubringen.

2.6 Die Europäische Datenschutz-Grundverordnung kommt – und die Unternehmen machen sich so ihre Gedanken

Im Berichtszeitraum wandte sich der Landesbeauftragte für den Datenschutz aus dem Saarland (LfD SL) an die Datenschutzbeauftragten des Bundes und der Länder. Grund hierfür war ein Schreiben eines extern bestellten Datenschutzbeauftragten (bDSB) an den LfD SL, der für ein deutschlandweit vertretenes Aktenvernichtungsunternehmen tätig sei. Der bDSB stellte das Unternehmen als renommierten und seriösen „Premium-Dienstleister“ im Bereich der Akten- und Datenträgervernichtung, der Archivierung und der Digitalisierung (wie Scan-Dienste) sowie als einen Garant für vorbildlichen Datenschutz und Datensicherheit vor. Das Unternehmen sieht sich als Mithelfer seiner Kunden und der Aufsichtsbehörden für den Datenschutz, um die Persönlichkeitsrechte der Betroffenen zuverlässig zu schützen. Der bDSB bat darum, die Verarbeitungsvorgänge Vernichtung, Archivierung und Digitalisierung von personenbezogenen Daten in die Liste gemäß Art. 35 Abs. 4 Datenschutz-Grundverordnung (DS-GVO), nach dem eine Datenschutzfolgeabschätzung durchzuführen ist, aufzunehmen. Danach ist in den Fällen, in denen die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte,

eine Rechtmäßigkeitsprüfung durchzuführen. Kernpunkt ist darin eine Auflistung der geplanten Abhilfemaßnahmen, durch die der Schutz der personenbezogenen Daten sichergestellt wird und damit die Risiken für die Betroffenen eingedämmt werden. Insbesondere wird die Erbringung eines Nachweises gefordert, dass die DS-GVO eingehalten wird. Der bDSB meint, dass die Verarbeitungsvorgänge der Vernichtung, Archivierung und Digitalisierung personenbezogene Daten beinhalten, die grundsätzlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen und in der Regel eine Datenschutz-Folgenabschätzung durchgeführt werden sollte. Mit der Aufnahme dieser Verarbeitungen in die o. g. Positivliste wäre dies für die Verantwortlichen vorgegeben.

Die Landesbeauftragten des Bundes und der Länder tauschten sich über die Einschätzung des bDSB aus. Da die Zentrale des Unternehmens, für das der bDSB tätig war, ihren Hauptsitz in Hamburg hat, wurde der hamburgische Datenschutzbeauftragte gebeten, stellvertretend für alle Datenschutzbeauftragten dem bDSB zu antworten. Dem bDSB wurde mitgeteilt, dass das angesprochene Thema, die Erarbeitung von Listen gemäß Art. 35 Abs. 4 und 5 zur Datenschutz-Folgenabschätzung, ausgesprochen wichtig sei und große praktische Bedeutung für die Unternehmen erlangen wird. Allerdings habe die Vorbereitung auf diese Problematik gerade erst begonnen. Deshalb könne zum jetzigen Zeitpunkt eine nähere Auseinandersetzung mit den Vorschlägen noch nicht erfolgen. Man könne jedoch davon ausgehen, dass insgesamt sehr deutliche Differenzierungen der aufzunehmenden Verarbeitungsvorgänge erforderlich würden. Die Anregungen des bDSB werden aber nicht verloren gehen und in die künftigen Überlegungen mit einfließen.

Eine Datenschutz-Folgenabschätzung (DSFA) hat gemäß Art. 35 Absatz 1 DS-GVO immer dann zu erfolgen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Weiterhin hat dann eine DSFA zu erfolgen, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese

in ähnlich erheblicher Weise beeinträchtigen. Auch bei der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche ist eine DSFA erforderlich. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die diese Datenschutz-Folgenabschätzung durchzuführen ist (sog. Blacklist) und veröffentlicht diese dann. Die deutschen Aufsichtsbehörden arbeiten derzeit mit Hochdruck an einer gemeinsamen Liste. Der Veröffentlichungszeitpunkt ist derzeit jedoch noch unbekannt.

2.7 Einbruchdiebstahl in der Kita

Im Berichtszeitraum informierte eine Kindertageseinrichtung (im folgenden Kita) über einen Einbruch und den Diebstahl sämtlicher Technik mit personenbezogenen Daten sowie digitalen Fotos. Die Eltern wurden sofort informiert. Die Kita bat über deren Träger den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Begleitung im Prozess der Aufklärung. Im ersten Schritt wollte der TLfDI wissen, welche technischen und organisatorischen Maßnahmen die Einrichtung getroffen hat, um diese Daten künftig zu schützen. Nach § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG) in Verbindung mit der Anlage zu § 9 Satz 1 haben nicht-öffentliche Stellen technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen, die erforderlich sind, um den Festlegungen des Gesetzes zu genügen. Hier geht es insbesondere darum, je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignete Maßnahmen zu treffen, Beispielsweise:

Zutrittskontrolle – Nach der Anlage zu § 9 BDSG sind unter der Zutrittskontrolle Maßnahmen zu verstehen, die verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden (z. B. Gebäudesicherung durch Zäune, Sicherung der Räume durch Sicherheitsschlösser, Chipkartenleser, Alarmanlagen, Codeschlösser usw.). Durch den Einbruchdiebstahl hatten Unbefugte Zutritt zur Kita und damit zur betreffenden Technik erlangt. Damit waren die ergriffenen Maßnahmen im Hinblick auf die Zutrittskontrolle nicht wirksam gewesen.

Zugangskontrolle – Nach der Anlage zu § 9 BDSG sind unter der Zugangskontrolle Maßnahmen zu verstehen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei allerdings das Wort „nutzen“ sich nicht auf die Legaldefinition des § 3 Abs. 5 BDSG beschränkt (z. B. Zugang zu Rechnern/Systemen, Authentifizierung, Benutzerkennung mit Passwort, Firewall, zertifikatsbasierte Zugangsberechtigung etc.). Durch den angezeigten Diebstahl könnten Unbefugte Zugang zu den gespeicherten personenbezogenen Daten erhalten.

Zugriffskontrolle – In Bezug auf die Zugriffskontrolle muss gewährleistet werden, dass die zur Benutzung von Datenverarbeitungsanlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind. Des Weiteren muss sichergestellt sein, dass personenbezogene Daten bei der Verarbeitung und Nutzung sowie nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können (z. B. Berechtigungskonzept, Benutzerkennung mit Passwort, gesicherte Schnittstellen etc.).

Weitergabekontrolle – Im Rahmen der Weitergabekontrolle muss verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

Eine Sicherung bei der elektronischen Übertragung kann zum Beispiel durch Verschlüsselung, VPN, Firewall, beim Transport mittels verschlossene Behälter und bei einer Übermittlung durch Verfahrensverzeichnis oder Protokollierungsmaßnahmen erfolgen.

Die Kita bezog daraufhin Stellung und teilte in Bezug auf die Zugangs- und Zugriffskontrolle mit, dass das Gebäude durch einen Zaun sowie eine zentrale Schließanlage gesichert ist. Eine Alarmanlage hat sich allerdings im Haus nicht befunden. Die Täter haben die Zaunanlage überstiegen und sind durch ein verschlossenes Fenster eingebrochen. Im Zuge der Einbruchsmeldung erfolgte mit der zuständigen Polizeidienststelle eine Begehung des Objektes. Diese hatte die Installation einer Alarmanlage empfohlen. Im Übrigen teilten die Zuständigen der Kita mit, dass sich zum Beispiel der Laptop in einem verschlossenen und mit Pincode versehenen Büroschrank befunden hatte. Der Laptop war mit einem Passwort geschützt. Dieses Passwort sei allen Mitarbeitern bekannt, die im Zuge ihrer Tätigkeit mit Dokumentationen und Auswertungen zu tun ha-

ben und diesen dadurch nutzen. Die einzelnen erfassten Dateien personenbezogener Daten waren auf dem gemeinschaftlich genutzten Laptop nicht nochmals separat verschlüsselt. Auf dem Laptop selbst war nicht ersichtlich, wer welche Daten zu welchem Zeitpunkt erfasst, verändert oder auch gelöscht hat. Dies könnte nur über die Dienstpläne nachvollzogen werden.

Auf die o. a. Probleme bezogen rät der TLfDI, die Zugriffe über eine entsprechende Dienstanweisung zu dokumentieren. So kann eindeutig nachvollzogen werden, wer den Laptop und die Daten genutzt hat. Der Laptop, der ausschließlich von der Einrichtungsleitung genutzt wurde, war ebenfalls mit einem Passwort versehen. Letzteres war alleine der Einrichtungsleitung bekannt. Stark zu bemängeln hatte der TLfDI, dass die personenbezogenen Daten auf beiden Laptops selbst nicht noch einmal geschützt worden sind. Hier wäre es ratsam, die Daten durch eine Festplattenverschlüsselung extra zu sichern und somit noch besser vor unbefugtem Zugriff zu schützen.

Die Kindertageseinrichtung folgte dem Rat des TLfDI und installierte eine entsprechende Software auf den Laptops.

Auch wenn die Schäden des Diebstahls im vorliegenden Fall nicht mehr rückgängig zu machen sind, so ist die Kindertageseinrichtung nun ein ganzes Stück besser aufgestellt, um alle personenbezogenen Daten besser zu schützen.

Nach § 9 Abs. 1 BDSG sowie der Anlage zu § 9 Satz 1 haben nicht-öffentliche Stellen technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen, die erforderlich sind, um den Festlegungen des Gesetzes zu genügen. Hier geht es insbesondere darum, je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignete Maßnahmen zu treffen.



Papierschnitzel Stichwort Kundenliste - ©Gina Sanders / Fotolia.com

3 Umgang mit Kundendaten

- 3.1 Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig!

Nun liegt er vor: Der 739 Seiten umfassende **Zwischenbericht des Untersuchungsausschusses** (UA) 6/2 zur Causa Immelborn (Drucksache 6/4641 v. 23. Oktober 2017), der das **rechtmäßige Amtshilfeersuchen** des TLfDI und dessen **rechtmäßiges Vorgehen** in der Aktenlager-Angelegenheit feststellt sowie die **skurrilen Vorgänge im Thüringer Innenministerium** offenlegt inklusive der **rechtswidrigen Ablehnung des Amtshilfeersuchens**.

Die Plenardebatte offenbarte zudem, dass die CDU im Untersuchungsausschuss ein externes Rechtsgutachten zu sämtlichen Rechtsfragen einholen wollte. Diese Idee scheiterte indes wiederum an der **Justiz**, die es für **offensichtlich abwegig** hielt, die **Aufgabe des Untersuchungsausschusses**, nämlich zu ermitteln und zu bewerten, auf einen externen Gutachter zu verlagern.

Der Untersuchungsausschuss gelangt überdies zu dem Ergebnis: Der von der CDU-Fraktion geäußerte Verdacht, der TLfDI habe die Klage auf Amtshilfe erhoben, um im Wahlkampf der TIM-Hausleitung schaden zu wollen, hat sich nicht erhärtet (Zwischenbericht, Rn. 1041).

Wer Interesse daran hat, nachzulesen, auf welchen krummen Wegen die CDU-Hausleitung des Innenministeriums gezielt, unter Verken-
nung vorliegender Rechtsgutachten und in rechtswidriger Weise
darauf hingewirkt hat, dem TLfDI die Amtshilfe zu versagen, der sei
auf die Rn. 1031 ff. des Zwischenberichts verwiesen.

Das Sondervotum der CDU-Fraktion finden Sie auf den Sei-
ten 727 ff.

**Der TLfDI dankt der Thüringer Polizei für ihre korrekte Bereit-
schaft zur rechtmäßigen Amtshilfe bei dem Mammut-Projekt
Aktenlager-Immelborn.**

3.2 Nerviges Meinungsforschungsinstitut

Den Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit erreichte eine Beschwerde über aufdringliche Werbeanrufe durch ein Meinungsforschungsinstitut an eine private Telefonnummer, die nicht im Telefonbuch gespeichert war.

Daraufhin wandte der TLfDI sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an das Meinungsforschungsinstitut mit der Bitte um Stellungnahme zu den datenschutzrechtlich relevanten Abläufen im Unternehmen (z. B. Generierung der Kontaktinformationen, Speicherung der Daten). Ebenso fragte der TLfDI nach der Melderegisteranmeldung gem. § 4d BDSG.

Das Unternehmen teilte dem TLfDI mit, dass es als Markt- und Sozialforschungsinstitut telefonische Umfragen in ganz Deutschland durchführe. Hierbei würden keine Verkaufsgespräche geführt. Es hätte jedoch vermehrt Probleme mit dem Missbrauch seiner Telefonnummer, was zu gehäuften Beschwerden führte. Darüber sei auch schon mit der Polizei gesprochen worden.

Zu den Verfahren äußerte sich das Unternehmen folgendermaßen: Die Telefonnummern würden dem Telefonbuch entnommen, wobei

die letzten beiden Ziffern nach dem Last-Digit-Verfahren per Zufall ersetzt werden. Sobald eine Kontaktperson die Teilnahme an einer Umfrage verweigere, würde die Rufnummer auf eine Sperrliste gesetzt, damit diese nicht mehr im Nummernpool für weitere Anrufe gespeichert sei. Außerdem gab das Unternehmen an, dass keine Melderegisterpflicht nach § 4d BDSG bestehe, da es einen betrieblichen Datenschutzbeauftragten bestellt hätte und keine personenbezogenen Daten verarbeiten würde. Da dies nicht alle aufgeworfenen Fragen klärte, entschied sich der TLfDI zu einer Vor-Ort-Kontrolle der automatisierten Datenverarbeitung.

Während der Kontrolle wurde das Markt- und Sozialforschungsinstitut darauf hingewiesen, dass gem. § 4g Abs. 4 BDSG Unternehmen, die mithilfe von automatisierten Verarbeitungen geschäftsmäßig personenbezogene Daten für Zwecke der Markt- und Meinungsforschung speichern, grundsätzlich verpflichtet sind, dies zu melden. Des Weiteren erhebt das Unternehmen durch die vorgenommene Generierung der Telefonnummern sehr wohl personenbezogene Daten. Gem. § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Bei Telefonnummern handelt es sich zumindest um Einzelangaben einer bestimmbar Person, da trotz Weglassens des Namens und der Anschrift des Betroffenen dieser immer noch bestimmbar bleibt. Da die Telefonnummern in einem Block zu dem dazugehörigen Projekt gespeichert werden, verarbeitet das Unternehmen auch personenbezogene Daten. Die Speicherung der Nummern erfolgt jedoch getrennt von der Speicherung der Interviewantworten, womit das Unternehmen den Anforderungen bei der geschäftsmäßigen Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung aus § 30 a BDSG nachkommt.

Das Markt- und Sozialforschungsinstitut wurde aufgefordert, seiner Meldepflicht nachzukommen, der es auch folgte.

Der Versuch des Auffindens der Telefonnummer des Beschwerdeführers in der Sperrliste blieb erfolglos. Auch stellte sich heraus, dass das Unternehmen zu dem Zeitpunkt des Anrufes keine Befragungen in diesem Ortsbereich durchgeführt hatte. Dies legte den Schluss nahe, dass es sich vorliegend doch um ein Problem mit dem Missbrauch der Telefonnummer des Unternehmens handelte und die störenden Anrufe nicht durch das Meinungsforschungsunternehmen selbst generiert worden sind.

Gemäß § 4d Abs. 1 BDSG sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht-öffentlichen Stellen der zuständigen Aufsichtsbehörde, sprich dem TLFDI, zu melden. Die Anforderungen für geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Markt- oder Meinungsforschung sind in § 30a BDSG normiert.

3.3 Daten-Theater

Eine Bürgerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz (TLFDI). In der Vorweihnachtszeit hatte sie Theaterkarten gekauft, um diese zu verschenken. Beim Kauf der Karten wurde sie nach ihrem Namen, der Anschrift und ihrer Telefonnummer gefragt, was sie schon seltsam fand. Auf ihre Frage, warum sie diese Angaben machen müsse, bekam sie an der Kasse die Antwort, dass man ihre Daten benötige, falls es zu einer Absage der Veranstaltung kommen würde. Ein Vierteljahr später kamen die Beschenkten zur Veranstaltung. Am Einlass wurden sie nach ihrem Namen gefragt, der, wie man sich denken kann, natürlich nicht auf der internen Anwesenheitsliste des Veranstalters zu finden war. Sie nannten dann den Namen ihrer Bekannten. Diese fand den Abgleich ihres Namens auf der Anwesenheitsliste merkwürdig und fragte nunmehr schriftlich beim Veranstalter an, warum ihre personenbezogenen Daten erhoben bzw. abgeglichen worden waren. Sie forderte den Veranstalter auf, ihre Daten zu löschen. Dieser Forderung und der Beantwortung ihrer Fragen kam der Veranstalter bis zum Zeitpunkt des Anschreibens an den TLFDI nicht nach.

Der TLFDI ist nach § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde über die Einhaltung des BDSG sowie anderer Vorschriften über den Datenschutz nach § 38 Abs. 1 BDSG bei nicht-öffentlichen Stellen. In dieser Funktion wandte er sich mit einem Auskunftersuchen an den Veranstalter. Er forderte den Veranstaltungsservice auf, unter Einhaltung von Fristen mitzuteilen, wie er mit den personenbezogenen Daten seiner Kunden umgeht. Er fragte weiter nach, in welcher Art und Weise die Käuferdaten erhoben und für welchen Zweck diese personenbezogenen Daten verwendet werden und wie die Löschung dieser Daten erfolgt. Nach

dem Eingang der erforderlichen Informationen kam der TLfDI zu folgender datenschutzrechtlicher Einschätzung:

Grundsätzlich muss es den Käufern möglich sein, Eintrittskarten für Veranstaltungen ohne Angabe ihrer personenbezogenen Daten zu erwerben. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in- oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sogenanntes Verbot mit Erlaubnisvorbehalt). Eine gesetzliche Grundlage zur Erhebung der Käuferdaten liegt nicht vor. Die personenbezogenen Daten der Käufer sind weder für die Begründung, Durchführung oder Beendigung des rechtsgeschäftlichen Schuldverhältnissen noch zur Wahrung ihrer berechtigten Interessen erforderlich, § 28 Abs. 1 Nr. 1 und 2 BDSG. Selbst wenn berechnigte Interessen dargelegt werden, überwiegen in jedem Fall die schutzwürdigen Interessen der Käufer an dem Ausschluss der Datenerhebung. Jedenfalls bei Barzahlung und bei Nutzung der üblichen Bezahlverfahren (EC-Karte, Kreditkarte) beim Kauf von Eintrittskarten ist die Erhebung der Käuferdaten nicht erforderlich. Lediglich bei Zahlung per Rechnung ist die Angabe der Adressdaten notwendig.

Eine solche Erforderlichkeit lässt sich auch hier nicht mit organisatorischen Gründen begründen. Zum einen sind die Käufer der Veranstaltungstickets oftmals nicht die Besucher der Veranstaltungen. Auch ist es nicht unüblich, die Karten bei Krankheit oder Urlaub an Freunde/Bekannte weiter zu verschenken. Zum anderen würde zu organisatorischen Gründen auch die reine Anzahl der Gäste einer Gruppe ausreichen. Deshalb stellte sich die Frage, weshalb die beim Kartenverkauf erhobenen Daten beim Einlass der jeweiligen Veranstaltung mit den Daten der Eingelassenen abgeglichen werden. Die Besucher können sich auch ohne Angabe ihres Namens, zum Beispiel unter Angabe der Personenzahl, ihre Plätze oder Tische aussuchen. Diese Zuordnung kann über beim Kauf vergebene Nummern erfolgen. Gerade bei Beschenkten führt die Namensangabe nicht zum Ziel und kann auch nicht mit einer internen Liste abgeglichen werden. Gleiches gilt für die Besucher, welche die Eintrittskarten von Beschenkten bekommen haben. Da hier keine gesetzliche Grundlage für die Erhebung der personenbezogenen Daten der Käufer vorliegt und diese Erhebung auch nicht für einen Veranstaltungsbesuch erforderlich ist, kommt daher nur eine Datenerhebung aufgrund der Einwilligung der Käufer in Betracht.

Diese Einwilligung der Käufer ist wiederum nur wirksam, wenn sie auf deren freien Entscheidung beruht und schriftlich erfolgt, § 4a Abs. 1 BDSG. Wenn der Kartenverkauf schon an die Bedingung der Preisgabe von Käuferdaten geknüpft ist, ist diese Einwilligung unwirksam. Die Käufer sind vor der Angabe ihrer personenbezogenen Daten darauf hinzuweisen, dass deren Angabe freiwillig erfolgt und für welche Zwecke diese erhoben werden. Die personenbezogenen Käuferdaten sind spätestens dann zu löschen, wenn sie nicht mehr erforderlich sind. Im Regelfall ist dies nach dem Ende einer jeden Veranstaltung der Fall. Der Löschvorgang wird in § 3 Abs. 4 Nr. 5 BDSG näher beschrieben und umfasst das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nach Angaben des Veranstaltungsservices ist es den Käufern zukünftig grundsätzlich möglich, Eintrittskarten für Veranstaltungen ohne Angabe ihrer personenbezogenen Daten zu erwerben. Soweit seitens des Veranstalters doch personenbezogene Daten der Käufer erhoben werden, erfolgt dieses zukünftig mit der Einwilligung der Käufer. Diese Einwilligung der Käufer basiert nunmehr auf deren freien Entscheidung und erfolgt schriftlich im Sinne des § 4a Abs. 1 BDSG. Die dem TLfDI dazu vorgelegte datenschutzrechtliche Mustereinwilligung wurde überprüft und entsprach nunmehr den datenschutzrechtlichen Bestimmungen.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt).

3.4 Der Anwalt als Datenschleuder?

Im Juni 2016 bat ein Veranstaltungsunternehmen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um datenschutzrechtliche Überprüfung, ob das Übermitteln von Kundendaten des Unternehmens und seiner anwaltlichen Prozessvertreter an Dritte, im vorliegenden Fall an das Gericht, im Rahmen eines Klageverfahrens gegen die Grundsätze des Datenschutzes verstoße. Nach Auffassung des Unternehmens würden die Betroffenen durch die Übermittlung dieser Daten in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Dies erwecke den

Eindruck, dass die betroffenen Unternehmenskunden ebenfalls am verfahrensgegenständlichen, auf Schadenersatz gerichteten Verhalten ihres Mandanten beteiligt gewesen seien. Darüber hinaus nutze das Veranstaltungsunternehmen diese personenbezogenen Daten zur rechtsmissbräuchlichen Verfolgung eigener Interessen.

Der TLfDI konnte nach Überprüfung des Sachverhalts keinen datenschutzrechtlichen Verstoß feststellen. Ein Eingriff in das Recht der informationellen Selbstbestimmung der betroffenen Kunden lag nach seiner Auffassung nicht vor.

Der TLfDI begründete seine Auffassung folgendermaßen: Die nicht-öffentlichen Stellen, unter die auch die Anwaltskanzlei fällt, müssen die Übermittlung personenbezogener Daten grundsätzlich an § 28 Abs. 1 BDSG ausrichten. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke unter bestimmten, in Abs. 1 aufgeführten Voraussetzungen zulässig.

Im vorliegenden Fall ergibt sich die Erlaubnis für die Übermittlung der Daten aus § 28 Abs. 1 Nr. 2 BDSG. Danach ist das Erheben und Übermitteln personenbezogener Daten zulässig, „... soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt...“. Im Sinne von § 28 Abs. 1 Nr. 1 ist es für die Erfüllung der Geschäftszwecke des Anwalts – die effektive Vertretung seiner Mandantschaft – erforderlich, personenbezogene Daten an das Gericht zu übermitteln. Vorliegend werden die Kundendaten an das Gericht zum Zweck der Betreuung des Mandatsverhältnisses als Beweisangebot gegenüber dem Gericht übermittelt. Nach dem BDSG liegt ein berechtigtes Interesse schon immer dann vor, wenn es sich aus vernünftigen Überlegungen ergibt und die vorgesehene Datenverwendung und der damit verfolgte Zweck im Einklang mit der Rechtsordnung stehen. In diesem Rahmen kommen sowohl ideelle als auch wirtschaftliche Interessen in Betracht. Ein rechtliches Interesse wird hierbei nicht vorausgesetzt, fällt jedoch stärker ins Gewicht (vgl. Dammann in Simitis, Kommentar zum BDSG, § 16 Rn. 17, 26).

Gerade die Wahrnehmung der rechtlichen Interessen des Mandanten stellt für die Anwaltskanzlei ein berechtigtes, qualifiziertes Interesse im Sinne des BDSG dar. Die Verfolgung der Rechte des Mandanten hängt im vorliegenden Fall von der Kenntnis der personenbezogenen

Daten der Kunden ab. Ohne diese Kenntnis wären ein Antrag auf Zeugenvernehmung nach § 373 ff. Zivilprozessordnung (ZPO), ein bestimmter Klageantrag mit den anspruchsbegründenden Voraussetzungen im Sinne des § 253 ZPO und dadurch letztendlich überhaupt die Geltendmachung des Schadensersatzanspruchs nicht möglich. Weiterhin sind die Parteien im Zivilprozessrecht verpflichtet, den Sachverhalt darzulegen und mögliche Beweise beizubringen.

Sofern die Anwaltskanzlei personenbezogene Daten verwendet, die sich auf „Gegner“ bzw. Betroffene beziehen, ist auch eine Interessenabwägung vorzunehmen. Die besondere Rolle des Rechtsanwalts nach dem BDSG wird hierbei dahingehend berücksichtigt, dass sogar „besondere Arten“ personenbezogener Daten nach § 3 Abs. 9 BDSG verarbeitet werden dürfen, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, § 28 Abs. 6 Nr. 3 BDSG.

Es wäre nicht nachvollziehbar, wenn ein Rechtsanwalt keine personenbezogenen Daten zur Begründung seiner Klageschrift an das Gericht übermitteln dürfte. Daher stehen im vorliegenden Fall keine schutzwürdigen Interessen der Betroffenen der Datenübermittlung an das Gericht entgegen.

Im Rahmen eines Klageverfahrens dürfen der bzw. die (anwaltlichen) Prozessvertreter im Rahmen des gerichtlichen Verfahrens personenbezogene Daten an das Gericht übermitteln, da dies i. d. R. zur Begründung der Klageschrift und im Verfahrensgang zur Aufklärung des Rechtsstreits erforderlich ist. Die Rechtsgrundlage ergibt sich aus § 28 Abs. 1 Nr. 2 BDSG und der Betreuung des Mandatsverhältnisses. Die Datenübermittlung erstreckt sich auch auf „besondere Arten“ personenbezogener Daten nach § 3 Abs. 9 BDSG. In diesen Fällen muss jedoch ganz besonders vorsichtig abgewogen werden und nicht erforderliche Informationen müssen sorgfältig geschwärzt werden.

3.5 Reparatur inklusive Datenverlust – wer richtig liest, erspart sich viel Ärger

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vom Landes-

beauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Beschwerde einer Bürgerin zuständigkeitshalber weitergeleitet. Die Bürgerin hatte ihr Notebook zur Instandsetzung im gekauften Markt abgegeben. Dabei hatte die Bürgerin ausdrücklich darauf hingewiesen, dass das Notebook lediglich hardwareseitig repariert werden solle, jedoch aber keine Software-Updates o. ä. durchgeführt werden sollen.

Nach Erhalt des Gerätes stellte die Bürgerin allerdings fest, dass Updates durchgeführt wurden und sämtliche persönlichen Daten nun gelöscht waren. Anhand der vorliegenden Fakten war eine Bearbeitung seitens des TLfDI noch nicht möglich. Er wandte sich deshalb an die Bürgerin und bat um Übersendung der allgemeinen Geschäftsbedingungen zu Reparaturaufträgen des Marktes.

Zeitgleich wandte sich der TLfDI an das Unternehmen, welches die Reparatur für den Elektronikmarkt durchführte und bat diesbezüglich um Stellungnahme. Das Unternehmen erklärte, dass für jede Reparatur eine Einsendungsbedingung für Garantiereparaturen durch den Kunden unterzeichnet wird und hierin klar definiert ist, dass die Daten durch die Kunden vor Abgabe zu sichern sind. Ebenso wird darauf hingewiesen, dass bei Bedarf nach den Reparaturen ein neues Update aufgespielt wird, falls die Qualitätskontrolle nicht erfolgreich war und der Kunde nach jeder Reparatur ein Recht auf ein einwandfrei funktionierendes Gerät hat. Im Falle eines solchen Updates könnten die Daten nicht wieder beschafft werden. Weiterhin wurde erklärt, dass es für die Reparaturaufträge einen Vertrag zur Datenverarbeitung im Auftrag gibt. Dabei handelt es sich um einen Vertrag, nach dem die weisungsgebundene Datenverarbeitung durch Externe – also nicht durch den Elektronikmarkt selbst, sondern durch einen Dritten – geregelt wird. Die Voraussetzungen für einen solchen Vertrag sind in § 11 Bundesdatenschutzgesetz (BDSG) geregelt. Bei einem wirksamen Abschluss können so personenbezogene Daten zwischen den Vertragspartnern – für den Geltungsbereich des Vertrages – ausgetauscht werden, ohne dass es eines gesetzlichen Erlaubnistatbestandes bedarf. § 11 BDSG beschreibt im Detail, welche Rechte, Pflichten und Maßnahmen im Einzelnen durch Vertrag zwischen Auftraggeber und Auftragnehmer zu treffen sind. Die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt dabei beim Auftraggeber.

Nach Sichtung der eingegangenen Unterlagen zu den Geschäftsbedingungen für Garantiereparaturen durch die Bürgerin, konnte sich der TLfDI ein abschließendes Bild machen.

Wie schon von dem Unternehmen mitgeteilt, unterzeichnete die Bürgerin die Einsendungsbedingungen für Garantiereparaturen. In diesen steht – wie bereits oben beschrieben – dass die Kunden dafür Sorge zu tragen haben, dass alle Daten vor Abgabe des Gerätes zur Reparatur gesichert werden sollten. Da es einen Vertrag über die Auftragsdatenverarbeitung gab, konnten bei der Verarbeitung der Daten durch das Unternehmen im Zuge dieser Reparaturen keine datenschutzrechtlichen Mängel festgestellt werden.

Hier gab es für den TLfDI nichts zu beanstanden.

Bei Reparaturaufträgen ist es ratsam, auch das Kleingedruckte zu lesen. Damit umgeht man böse Überraschungen. Nicht nur im Hinblick auf wichtige persönliche Unterlagen, sondern auch auf private Erinnerungsfotos wäre es schade, wenn diese wegen einer kleinen, aber durchaus weitreichenden Unachtsamkeit verloren gehen würden.

3.6 Datenerhebung zur Beitreibung rechtmäßiger offener Forderungen ist kein Datenschutzverstoß

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Autohaus. Er trug vor, dass die Mitarbeiter einer Abschleppfirma des Autohauses seine persönlichen Daten missbraucht und Freiheitsberaubung begangen hätten. Der Beschwerdeführer legte dar, dass er im Parkhaus eines Krankenhauses auf dem Parkplatz des medizinischen Notdienstes geparkt habe und das Auto bei seiner Rückkehr mit einer Parkkralle versehen gewesen sei. Der Mitarbeiter der Abschleppfirma, der die Kralle angebracht hatte, forderte zur Auslösung des Fahrzeugs 50,00 € vom Beschwerdeführer und bezog sich dabei auf eine entsprechende Weisung seines Vorgesetzten, diese Zahlung einzufordern. Der Beschwerdeführer konnte bzw. wollte die 50,00 € jedoch nicht zahlen. Daraufhin habe der Mitarbeiter des Autohauses die Unterzeichnung eines Formulars zur Angabe von Name und Anschrift des Fahrzeughalters gefordert. Dieses Formular habe der Beschwerdeführer ausgefüllt und unterzeichnet. Dennoch habe der Mitarbeiter der Abschleppfirma auch noch den Personalausweis und

die Fahrzeugzulassung des Beschwerdeführers gefordert, um sie zu fotokopieren. Der Beschwerdeführer bezweifelte, dass die Fotodokumentation seiner amtlichen Dokumente rechtmäßig erfolgte und betonte, dass der Mitarbeiter der Abschleppfirma ihn insofern erpresst habe, da er sonst die Parkkralle nicht entfernt hätte. Er bat den TLfDI, diesen Sachverhalt datenschutzrechtlich zu prüfen und das Verhalten des Autohauses ggf. zu ahnden.

Der TLfDI hat das Autohaus um eine Stellungnahme zum vorgetragenen Sachverhalt hinsichtlich der Fotodokumentation des Personalausweises und der Zulassung im Rahmen des Abschleppvorgangs gebeten.

Das Autohaus teilte dem TLfDI mit, dass zum dargelegten Abschleppvorgang keine Bilder, Scanner-Dateien oder Ähnliches vorhanden seien. Seine Erklärung belegte das Autohaus glaubhaft mittels Screenshots der elektronischen Akte des Vorgangs.

Weiterhin teilte das Autohaus dem TLfDI mit, dass es vonseiten des Unternehmens den Abschleppfahrern grundsätzlich untersagt ist, Aufnahmen von Personalausweisen anzufertigen. Zum Zweck der Erfassung von personenbezogenen Daten lassen sich die Abschleppfahrer lediglich den Personalausweis und die Fahrzeugzulassung des Fahrzeugführers vorlegen. Die Fahrer schreiben diese Daten aus den vorgelegten Dokumenten ab und erfassen sie auf dem Auftrag und in der Kundendatei. Als Beleg übersandte das Autohaus dem TLfDI einen Abdruck aus der Kundendatei zum vorgetragenen Sachverhalt. Hieraus war ersichtlich, dass der Abschleppfahrer tatsächlich keine weiteren Daten erfasst hatte.

Aufgrund der Stellungnahme des Autohauses teilte der TLfDI dem Beschwerdeführer mit, dass die Mitarbeiter des Abschleppdienstes im Auftrag des Autohauses lediglich Namen, Anschrift und Geburtsdatum erfassten, um offene Forderungen beizutreiben. Dies begründet jedoch keinen Verstoß gegen datenschutzrechtliche Vorgaben. Gemäß § 28 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben personenbezogener Daten oder ihre Nutzung zulässig, wenn ihre Kenntnis zur Erfüllung eigener Geschäftszwecke dient – im vorliegenden Falle zur Beitreibung offener Forderungen des Abschleppdienstes. Gemäß § 28 Abs. 1 Satz 2 BDSG muss der Zweck, für den die Daten erhoben werden, genau angegeben sein, beispielsweise für die Begleichung offener Zahlungsforderungen. Im vorliegenden Falle bestanden keine Anhaltspunkte dafür, dass das Abschleppunternehmen des Autohauses gegen die datenschutzrechtli-

chen Regelungen verstoßen hatte. Somit hatten die Mitarbeiter des Abschleppdienstes nicht rechtswidrig in das Recht des Beschwerdeführers auf informationelle Selbstbestimmung eingegriffen. Parallel dazu informierte der TLfDI das Autohaus darüber, dass kein datenschutzrechtlicher Verstoß festgestellt werden konnte.

Gemäß § 28 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben personenbezogener Daten oder ihre Nutzung zulässig, wenn ihre Kenntnis zur Erfüllung eigener Geschäftszwecke dient – im vorliegenden Falle zur Beitreibung offener Forderungen des Abschleppdienstes. Gemäß § 28 Abs. 1 Satz 2 BDSG muss der Zweck, für den die Daten erhoben werden, genau angegeben sein. Somit stellt die Abschrift von Name, Anschrift und Geburtsdatum aus amtlichen Dokumenten (Personalausweis, Kfz-Zulassung) zur Beitreibung rechtmäßiger offener Forderungen keinen Verstoß gegen datenschutzrechtliche Vorgaben und keinen Eingriff in die informationelle Selbstbestimmung des Dokumenteninhabers dar.

3.7 Bewerbung erfolglos – Daten löschen!

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Beschwerde eines Bürgers vor. Dieser hatte sich per E-Mail mit einem Auskunftersuchen nach § 34 Bundesdatenschutzgesetz (BDSG) unter Fristsetzung an ein Thüringer Autohaus gewandt. Hintergrund seines Auskunftersuchens war seine vorangegangene Bewerbung bei diesem Unternehmen. Auf das geforderte Auskunftersuchen sei seitens des Autohauses keine Reaktion erfolgt, so der Beschwerdeführer.

Der TLfDI wandte sich mit einem Anschreiben an das Autohaus. Er wies daraufhin, dass nach § 34 Abs. 1 Nr. 1 bis 3 BDSG die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten, die Herkunft der Daten, den Empfänger der Daten oder die Kategorie von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung zu erteilen hat. Darüber hinaus machte er den Geschäftsführer darauf aufmerksam, dass nach § 43 Abs. 1 Nr. 8a BDSG ordnungswidrig handelt, wer vorsätzlich oder fahrlässig eine Auskunft nicht oder nicht rechtzeitig erteilt. Eine solche Ordnungswidrigkeit kann nach § 43 Abs. 3 BDSG mit einer Geldbuße von bis zu 50.000 € geahndet werden.

Das Unternehmen wurde in diesem Zusammenhang unter Fristsetzung um Stellungnahme gebeten. Der externe Datenschutzbeauftragte des Unternehmens teilte dem TLfDI mit, dass er bereits vor geraumer Zeit dem Beschwerdeführer schriftlich mitgeteilt habe, dass keine personenbezogenen Daten über ihn im betreffenden Autohaus gespeichert sind. Er hatte auf das Auskunftsverlangen des Beschwerdeführers nochmals geantwortet und ausgeführt, dass ein entsprechender Datensatz – hier seine Bewerbung – nicht in den Datenverarbeitungssystemen des Autohauses, sowohl analog als auch digital, gefunden werden konnte. Zwar bestätigte eine Mitarbeiterin, dass von ihm in der Vergangenheit eine Bewerbung beim Autohaus per E-Mail eingegangen war. Diese wurde jedoch gleich nach Auswertung der eingegangenen Bewerbungen wieder gelöscht. Nachdem das Autohaus den Schriftverkehr mit dem Betroffenen dem TLfDI lückenlos nachweisen konnte und auch die Bestellurkunde des betrieblichen Datenschutzbeauftragten in Kopie vorlegte, sah der TLfDI den Vorgang aus datenschutzrechtlicher Sicht als erledigt an. Ein datenschutzrechtlich rechtswidriges Verhalten war insoweit nicht festzustellen.

Jeder Bewerber hat das Recht, dass seine Bewerberdaten nach Ablauf des Einstellungsverfahrens unverzüglich gelöscht werden. Datenschutzrechtlich ergibt sich diese Verpflichtung aus § 35 Abs. 2 Nr. 3 BDSG, wonach Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

3.8 Hotelinsolvenz: Gehören die Kundendaten dem neuen Eigentümer?

Ein ehemaliger Hotelbetreiber aus Thüringen bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft darüber, ob er als früherer Gesellschafter Kundendaten seines Hotels zurückbekommen könnte und inwiefern eine entsprechende Verfahrensweise rechtmäßig sei. Das Hotel hatte als Unternehmergesellschaft bestanden und der Betreiber musste einen Insolvenzantrag stellen. Im Rahmen des Insolvenzantrags wurde das Hotel von einem anderen Pächter übernommen und weitergeführt. Dabei seien nach Auskunft des ehemaligen Betreibers auch sämtliche Unterlagen und PCs mit gespeicherten Daten in den

Besitz des neuen Pächters übergegangen. Nach Aussage des ehemaligen Betreibers befanden sich darunter auch sämtliche Kundendaten des Hotels (ca. 6.000) sowie Kreditkarten- und Buchhaltungsdaten. Der TLfDI teilte dem ehemaligen Hotelbetreiber als Beschwerdeführer mit, dass eine mögliche Rückgabe der Daten aus seiner Sicht zivilrechtlich geklärt werden müsse. Der TLfDI wies daraufhin, dass er den vorgetragenen Sachverhalt vorbehaltlich genauerer Informationen jedoch datenschutzrechtlich bewerten wird. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei der „Übertragung“ von Kundendaten des Hotels auf den nachfolgenden Pächter handelt es sich um eine Datenübermittlung, die Teil der Datenverarbeitung ist. Gemäß § 4 Abs. 1 BDSG benötigt der Übermittler bzw. der Insolvenzverwalter eine entsprechende Rechtsgrundlage oder die Einwilligung der jeweiligen Kunden, um die Daten von einem Unternehmen auf das Folgeunternehmen zu übertragen.

Als Rechtsgrundlage kam im vorliegenden Fall allenfalls § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG in Betracht, da eine Weitergabe von Daten aufgrund einer Veräußerung des Unternehmens eine Zweckänderung darstellt. Gemäß § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig. Die Daten wurden zur Durchführung eines Beherbergungs- und Bewirtungsvertrages erhoben und gespeichert. Die Rechtsnorm zur Datenübermittlung gemäß § 28 BDSG setzt jedoch ein berechtigtes Interesse eines Dritten (Folgepächter) voraus. Im Hinblick darauf war für den TLfDI nicht ersichtlich, inwiefern ein solches Interesse vorliegt. Darüber hinaus darf gemäß § 28 Abs. 2 Satz 1 Nr. 2 BDSG kein Grund zur Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hat. Dies konnte nach Auffassung des TLfDI im vorliegenden Falle nur zutreffen, wenn die Betroffenen jeweils vor der Datenübermittlung an den neuen Pächter informiert wurden und eine Möglichkeit zum Widerspruch eingeräumt war.

Mit der Insolvenzeröffnung geht die Verwaltungs- und Verfügungsbefugnis auf den Insolvenzverwalter über. Dies betrifft alle Vermögensgegenstände des insolventen Unternehmens. Sobald der Insolvenzverwalter den intakten Unternehmensteil an einen anderen Un-

ternehmer veräußert hat, wechselt auch die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG. Der neue Unternehmer – vorliegend der neue Pächter – führt dann in aller Regel das Unternehmen fort oder integriert es in ein eigenes, bereits bestehendes Unternehmen. Erst wenn dies stattgefunden hat, wechselt die verantwortliche Stelle. Aufgrund der Informationen des Beschwerdeführers ging der TLfDI davon aus, dass das Insolvenzverfahren noch nicht abgeschlossen war und der Beschwerdeführer insofern noch als Gesellschafter des insolventen Unternehmens fungierte und damit verantwortliche Stelle im Sinne des BDSG war. Der TLfDI sah nach den ihm vorliegenden Informationen die Datenübermittlung zum neuen Pächter als rechtswidrig an. Daher bat er den Beschwerdeführer gemäß § 38 Abs. 3 BDSG um genauere Informationen zum Sachverhalt, insbesondere darüber, unter welchem Namen das Hotel geführt wurde, wer der neue Pächter war, von welchem Insolvenzverwalter das Insolvenzverfahren geführt wurde und wie der Verfahrensstand ist. Der Beschwerdeführer teilte dem TLfDI die erbetenen Auskünfte schließlich mit.

Nach § 4 Abs. 1 BDSG benötigte der bestellte Insolvenzverwalter eine Erlaubnissnorm oder die Einwilligung der jeweiligen Kunden, um die Daten an den neuen Pächter weiterzugeben. Daher bat der TLfDI den Insolvenzverwalter nach § 38 Abs. 3 BDSG um Stellungnahme zum Sachverhalt und um Information, inwiefern im Rahmen der Insolvenzabwicklung Unterlagen und PCs mit personenbezogenen Daten von Hotelgästen (Kreditkarten- und Buchhaltungsdaten), Mitarbeitern und weiteren Betroffenen in den Besitz des neuen Pächters übergegangen sind, auf welcher Rechtsgrundlage dies ggf. erfolgte und ob die betreffenden Kunden zuvor in die Datenübermittlung eingewilligt hatten. Weiterhin bat der TLfDI um Auskunft über die Art und Weise, wie das insolvente Unternehmen an den neuen Inhaber übergegangen ist, d. h., ob das alte Unternehmen fortgeführt oder ob ein neues Unternehmen gegründet wurde, das den (alten) Geschäftsbetrieb fortgeführt hat.

Parallel dazu bat der TLfDI den neuen Hoteleigner um eine Stellungnahme zu den aufgeworfenen Fragen und um folgende Auskünfte: In welcher Form wurde das Hotel an den neuen Pächter überschrieben, wurden die dabei übermittelten Kundendaten im Insolvenzverfahren gesondert verhandelt, auf welcher Rechtsgrundlage wurden diese Daten durch den neuen Pächter erhoben, wurden die jeweiligen Kunden über die Datenerhebung in Kenntnis gesetzt bzw.

haben sie hierin eingewilligt? Der neue Hoteleigner informiert den TLfDI darüber, dass er das Hotel käuflich erworben habe und verwies auf seinen beigelegten Kaufvertrag. Die Inhalte der PCs waren nach Auskunft des neuen Hoteleigners zuvor vollständig, bis auf das Hotelprogramm HS3, vom Insolvenzverwalter gelöscht worden. Alle Abrechnungen, Personalunterlagen und Dokumente, die die Angelegenheit vor der Übernahme durch den neuen Pächter betrafen, hatte der Insolvenzverwalter übernommen und archiviert.

Der Insolvenzverwalter bestätigte dem TLfDI die Übernahme des Hotels durch den neuen Pächter. Er dementierte jedoch, dass der neue Pächter über die Internetseite des Hotels gespeicherte personenbezogene Kundendaten von Hotelgästen der Schuldnerin erhalten hatte.

Aufgrund der vom Insolvenzverwalter gegebenen Informationen teilte der TLfDI dem Insolvenzverwalter die datenschutzrechtliche Erledigung der Angelegenheit mit. Weiterhin informierte der TLfDI den Beschwerdeführer und früheren Hoteleigner darüber, dass sowohl der Insolvenzverwalter als auch der neue Hoteleigner glaubhaft versichert hätten, dass keine Daten an den neuen Hotelbetreiber übermittelt worden seien. Insbesondere hätten keine gespeicherten Kreditkartendaten im insolventen Unternehmen vorgelegen.

Gemäß § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder deren Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig. Im Falle der Datenübermittlung darf gemäß § 28 Abs. 2 Satz 1 Nr. 2 BDSG kein Grund zur Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hat. Sobald ein Insolvenzverwalter im Rahmen des Insolvenzverfahrens den intakten Unternehmensteil an einen anderen Unternehmer veräußert hat, ändert sich auch die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG. Nach § 4 Abs. 1 BDSG benötigt der bestellte Insolvenzverwalter eine Erlaubnisnorm oder die Einwilligung der jeweiligen Kunden, um gespeicherte personenbezogene Daten an den neuen Unternehmenseigner weiterzugeben.

3.9 Das Probeabonnement einer Zeitung als Türöffner für Werbeattacken

Im Juli 2016 beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Thüringer Zeitung und teilte mit, dass er von einer Mitarbeiterin der Zeitung mit der Nummer +49 800 ... angerufen worden sei. Bei diesem Werbeanruf habe ihm die Mitarbeiterin ein kostenloses Probeabonnement der Zeitung angeboten. Die für den Werbeanruf verwendeten personenbezogenen Daten stammten nach Aussage der Mitarbeiterin aus einem bereits länger zurückliegenden Probeabonnement. Eine Einwilligung in die dauerhafte Speicherung oder in Werbeanrufe hatte der Beschwerdeführer der Zeitung jedoch nicht erteilt. Nach dem Werbeanruf hatte er die Zeitungsmitarbeiterin aufgefordert, seine personenbezogenen Daten zu löschen und wandte sich mit der Bitte um Überprüfung auf das datenschutzkonforme Verhalten der Zeitungsmitarbeiter an den TLfDI.

Der TLfDI wandte sich zunächst an die Mediengruppe, zu der auch die vorgenannte Zeitung gehörte, und bat um eine Stellungnahme zum Sachverhalt gemäß § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG). In ihrer Stellungnahme legte die Mediengruppe dar, dass der Beschwerdeführer über den Leserservice für den Zeitraum vom 8. März bis 18. März 2013 ein Probeabonnement einer Regionalausgabe der Zeitung bestellt und über die Bestellmaske seine Adress- und Kontaktdaten angegeben hatte. Weiterhin legte die Mediengruppe dar, dass sich im Bestellvorgang ein farblich hervorgehobener Datenschutzhinweis mit Werbeerlaubnis befände, den der Kunde selbst durch Setzen des Häkchens aktiviere und damit bestätige, dass er die Bedingungen gelesen habe und damit einverstanden sei.

Somit war auch der Beschwerdeführer im Rahmen des Bestellvorgangs für das Probeabonnement auf die Datenschutzrechte einschließlich der Möglichkeit zum Widerspruch hingewiesen worden. Die übersandte Aufforderung zur Überprüfung der Daten mit dem wiederholten und inhaltlich unveränderten Hinweis auf die Werbeerlaubnis hatte der Beschwerdeführer durch Anklicken des Buttons „JETZT BESTELLEN“ bestätigt.

Anschließend erhielt der Beschwerdeführer eine Bestellbestätigung, die sowohl seine angegebenen Kontaktdaten enthielt als auch einen erneuten Hinweis auf die Werbeerlaubnis (sog. Double-Opt-In-Verfahren). Nach Darlegung der Mediengruppe hatte der Beschwer-

deführer somit wirksam seine Einwilligung in die Nutzung seiner Daten erteilt und er hatte noch die Möglichkeit, die Bestellbestätigung auszudrucken. Der Leserservice übermittelte daraufhin per csv-Datei seine Bestellbestätigung an die Mediengruppe. Im Zeitraum 2013 bis 2016 folgten daraufhin unterschiedliche Briefwerbungen an die angegebene postalische Adresse des Beschwerdeführers.

Aufgrund der Stellungnahme der Mediengruppe prüfte und bewertete der TLfDI den Sachverhalt datenschutzrechtlich und teilte das Ergebnis auch der Mediengruppe mit. Da Double-Opt-In-Verfahren regelmäßig von verschiedenen Firmen verwendet werden und Kunden bei entsprechenden Newsletter-Anmeldungen zum Teil auch Rabatte zugesichert bekommen, bezog der TLfDI in seine Prüfung auch ein grundsätzliches Urteil des Landgerichts München ein.

Nach Auffassung des TLfDI behalten Opt-Ins nicht ewig ihre Gültigkeit. Generell gelten Einwilligungen für den jeweils beschriebenen Umfang. Solange sich der Empfänger nach dem Erhalt eines Newsletters nicht wieder austrägt, gilt seine Einwilligung für jede weitere Ausgabe des Newsletters. Erhält ein Empfänger eine Zeit lang keine Newsletter (mehr), ist davon auszugehen, dass die Einwilligung nicht mehr besteht. Wann dieser Zeitpunkt ist, hängt vom Einzelfall ab. Dazu hat das Landgericht (LG) München mit Urteil vom 8. April 2010 (Az. 17 HK O 138/10) festgestellt, dass die Einwilligung ihre Gültigkeit auch dann verlieren kann, wenn von ihr über einen längeren Zeitraum kein Gebrauch gemacht wird. Dies gelte unabhängig davon, ob die Einwilligung tatsächlich wirksam erteilt wurde. Begründet wird dies damit, dass der Adressat der E-Mail-Werbung nach einer bestimmten Zeit nicht mehr damit rechnen muss, dass er noch weitere Werbung erhalte. Damit würde dann der Zustand vor Erteilung einer Einwilligung eintreten. Somit würde der Versand einer werblichen E-Mail dann eine unzumutbare Belästigung nach § 7 Gesetz gegen den unlauteren Wettbewerb darstellen. Im vorliegenden Urteil hatte das Gericht keine konkrete Gültigkeitsdauer der Einwilligung benannt; es ging jedoch davon aus, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb keine rechtliche Grundlage mehr ist.

In Anlehnung an das Urteil des LG München kam auch der TLfDI zu der Auffassung, dass die im März 2013 erteilte Einwilligung des Beschwerdeführers ab August 2014 keine rechtliche Grundlage mehr darstellte, weder für Briefwerbung noch für telefonische Werbekon-

takte. Der TLfDI forderte die Mediengruppe auf, ihm mitzuteilen, dass die personenbezogenen Daten des Beschwerdeführers mittlerweile gelöscht wurden bzw. ob dessen Werbewiderspruch berücksichtigt wurde. Im November 2016 bestätigte die Mediengruppe gegenüber dem TLfDI schriftlich, dass der Werbewiderspruch berücksichtigt wurde. Seine personenbezogenen Daten wurden bis zum Ablauf der kaufmännischen Aufbewahrungspflichten gem. § 35 Abs. 3 Nr. 1 BDSG gesperrt. Nach Ablauf der Sperrfrist werden die Daten des Beschwerdeführers gelöscht. Gegen dieses Vorgehen hatte der TLfDI aus datenschutzrechtlicher Sicht keine Bedenken.

Sofern Kunden bei der Bestellung von Probeabonnements oder Probeprodukten per Opt-In-Verfahren die Einwilligung zu einer Werbeerlaubnis erteilen, ist diese Einwilligung nicht dauerhaft gültig. Erhält ein Empfänger eine Zeit lang keine Werbung (mehr), ist davon auszugehen, dass die Einwilligung nicht mehr besteht. In Anlehnung daran geht das Landgericht München davon aus, dass eine 17 Monate zurückliegende und bisher nicht genutzte Einwilligung zur E-Mail-Werbung nicht mehr aktuell und somit keine rechtliche Grundlage für entsprechende Werbung ist. Unabhängig davon ist die Frage, wann eine erteilte Einwilligung in Werbung ihre Gültigkeit verliert, im Einzelfall zu klären.

3.10 Baumarkt verlangt Adressangabe beim Umtausch

Ein Bürger hatte in einem Baumarkt eine 5-Kilo-Propangas-Flasche umgetauscht. Hierzu verlangte der Baumarkt von ihm, seinen Namen und seine Adresse in einem Formular anzugeben. Er war daraufhin verwundert und suchte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine plausible datenschutzrechtliche Erklärung, ob diese Datenerhebung überhaupt zulässig war.

Der TLfDI teilte dem Betroffenen daraufhin Folgendes mit: Gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als Rechtsgrundlage für die Erhebung und Speicherung von Kundendaten bei Umtausch oder Reklamation kommt hier § 28 Abs. 1 Nr. 1 BDSG in Betracht. Dort ist geregelt, dass das Erheben, Speichern, Verändern

oder Übermitteln personenbezogener Daten und ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Bei dem Kauf einer 5-Kilo-Propangas-Flasche und dem darauffolgenden Umtausch handelt es sich um einen Kaufvertrag zwischen dem Bürger als Käufer und dem Baumarkt als Verkäufer im Sinne des § 433 Abs. 1 Bürgerliches Gesetzbuch (BGB). Bei einem Umtausch oder einer Reklamation entsteht zwischen den jeweiligen Kunden und dem Einzelhandelsunternehmen ein sog. Rückabwicklungsschuldverhältnis. Für das Rückabwicklungsschuldverhältnis könnte es daher erforderlich sein, die Kundendaten zu erheben bzw. zu speichern. Diese Erforderlichkeit müsste der Baumarkt begründen können. Die Erforderlichkeit für die Erhebung der Kundendaten könnte sich bei einem Umtausch von Waren zum einen daraus ergeben, dass sich eventuell erst nachträglich feststellen lässt, ob die umgetauschte Ware beschädigt ist und dadurch ggf. Regressansprüche aus dem Rückabwicklungsverhältnis entstanden sind. Zum anderen kann dies nötig sein, um in diesem Zusammenhang auftretenden Manipulationen (Missbrauch, Unterschlagung von Geld) durch das Personal vorzubeugen. Oft werden heutzutage in Einzelhandelsunternehmen Waren auch ohne gültigen Kassenbon ohne jegliche weitere Prüfung oder Bewertung eines Anspruchs zurückgenommen und der Kaufpreis wird in bar zurückerstattet. Vor allem handelt es sich dabei um einen besonderen Service bzw. um Kulanz des entsprechenden Einzelhandelsunternehmens. Dafür verlangen die Unternehmen auch eine Bestätigung der Kunden, dass sie für die zurückgegebene Ware den Kaufpreis erstattet bekommen haben. So könnte auch der schon angesprochene Missbrauch durch Mitarbeiter verhindert oder möglicherweise eine begangene Unterschlagung nachgewiesen werden. Liegt eine solche Erforderlichkeit jedoch nicht vor, ist davon auszugehen, dass die Datenerhebung und mithin auch die Speicherung dieser Daten rechtswidrig wäre.

Da der Betroffene sich nicht damit einverstanden erklärte, dass sich der TLfDI an den Baumarkt unter Nennung seines Namens wendet, war es nicht möglich den Einzelfall vollumfänglich aufzuklären. Daher wurde der Fall allgemein betrachtet und dem Betroffenen wurden die Zusammenhänge erklärt.

Nach § 4 Abs. 1 BDSG ist grundsätzlich jeder Umgang mit personenbezogenen Daten nur dann möglich, wenn eine gesetzliche Vorschrift dies erlaubt oder eine Einwilligung des Betroffenen vorliegt. Im dargestellten Fall war einschlägige Rechtsvorschrift § 28 BDSG – Datenerhebung und -speicherung für eigene Geschäftszwecke. Hierfür muss eine der Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 1 bis 3 BDSG zutreffend sein, damit die Datenerhebung oder -speicherung von personenbezogenen Daten für eigene Geschäftszwecke zulässig ist.

3.11 Versteckte Einwilligungserklärung

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Berichtszeitraum durch eine anonyme Beschwerde darauf aufmerksam gemacht, dass in einem Hotel eine Datenschutzerklärung in der Gästemappe vorhanden war, welche nicht den datenschutzrechtlichen Bestimmungen entspreche. Durch Einschreiten des TLfDI konnten die Mängel hinsichtlich der Datenschutzerklärung aufgeklärt und abgestellt werden. Zudem verwendete das Hotel einen Meldeschein für Gäste, welcher ebenfalls nicht den Bestimmungen des Datenschutzes entsprach.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Rechtsgrundlage für die Erhebung der personenbezogenen Daten der Hotelgäste zur Registrierung ist § 29 Bundesmeldegesetz (BMG). Nach § 29 Abs. 2 BMG haben beherbergte Personen am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben, der die in § 30 Abs. 2 BMG aufgeführten Daten enthält. Hierzu gehören Datum der Ankunft und der voraussichtlichen Abreise, Familienname, Vorname, Geburtsdatum, Staatsangehörigkeiten, Anschrift, Zahl der Mitreisenden und ihre Staatsangehörigkeit, Seriennummer des anerkannten und gültigen Passes. Darüber hinaus hatte das Hotel weitere umfangreiche Daten auch betreffend der Familienangehörigen bzw. Mitreisenden erhoben. Dies war jedoch laut Bundesmeldegesetz und auch auf Grundlage keiner anderen Erlaubnisnorm erforderlich, die Daten konnten nur auf freiwilliger Basis erhoben werden. Daraufhin übersandte die verantwortliche Stelle einen überarbeiteten Meldeschein, welcher eine Datenschutzerklärung mit einer

Einwilligungserklärung zur Erhebung von personenbezogenen Daten enthielt, welche nicht gesondert hervorgehoben, sondern in die Datenschutzerklärung als Fließtext eingebunden wurde. Auch in der Überschrift fand sich kein Hinweis auf eine zu erteilende datenschutzrechtliche Einwilligung des Betroffenen. Zudem musste laut dem Formular die Einwilligung zusammen mit der zwingenden Unterschrift zum Meldeschein erfolgen. Ferner wurde eine sog. Opt-Out-Formulierung gewählt, wonach jederzeit der erteilten Einwilligung widersprochen werden kann. Nach § 4a Abs. 1 BDSG ist eine Einwilligung zusammen mit anderen abzugebenden schriftlichen Erklärungen besonders hervorzuheben. Datenschutzfreundlicher ist es auch, wenn die Einwilligung in einem separaten Kästchen mit separater Unterschrift auf einem Formular als sog. Opt In dargestellt würde. Eine versehentlich erteilte Einwilligung der Kunden und Gäste wäre faktisch ausgeschlossen. Der TLfDI stellt auf seiner Website die „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“ des Düsseldorfer Kreises als Hilfe bei der Formulierung Unternehmen zur Verfügung (https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/orientierungshilfe_zur_datenschutzrechtlichen_einwilligung.pdf)



Der TLfDI wies das Hotel auf die vorzunehmenden Änderungen hin, um eine datenschutzrechtlich wirksame Einwilligung der Betroffenen herbeizuführen. Die verantwortliche Stelle kam der Aufforderung des TLfDI im vollen Umfang nach.

Sofern die personenbezogenen Daten nicht auf Grundlage einer Rechtsvorschrift nach dem BDSG oder anderer Vorschriften über den Datenschutz erhoben und verarbeitet werden können, ist eine Einwilligung der Betroffenen erforderlich, § 4 Abs. 1 BDSG. Die von Unternehmen zumeist verwendeten datenschutzrechtlichen Einwilligungserklärungen in die Datenerhebung und -verarbeitung von personenbezogenen Daten entspricht zumeist nicht den Vorgaben des § 4a Abs. 1 BDSG. Hierfür hat der Düsseldorfer Kreis eine „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in entsprechenden Formularen“ zur Verfügung gestellt

(https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/orientierungshilfe_zur_datenschutzrechtlichen_einwilligung_.pdf).

3.12 Pkw-Stellplatz gegen Ausweiskopie – was ist in der Mieter-selbstauskunft zulässig?

Im Januar 2016 beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Unternehmen für Gebäudeservice im Rahmen einer Mieter-selbstauskunft für einen Stellplatz verlangte, eine Kopie vom Personalausweis oder Reisepass abzugeben. Der Beschwerdeführer hatte diese Kopie mit Verweis auf den Datenschutz verweigert. Daraufhin leitete die Firma seine Mietanfrage wegen fehlender Unterlagen nicht weiter, sodass kein Mietvertrag zustande kam. Weiterhin vermutete der Beschwerdeführer, dass das Serviceunternehmen die hohen Anforderungen zur Speicherung und Aufbewahrung von sensiblen personenbezogenen Daten gar nicht erfüllen kann.

Daher wollte der Beschwerdeführer vom TLfDI wissen, wer die korrekte Aufbewahrung von personenbezogenen Daten kontrolliert, ob Firmen eine Kopie des Personalausweises von Kunden verlangen dürfen und ob nicht-öffentliche Stellen personenbezogene Daten von Kunden überhaupt erheben dürfen? Falls Firmen dies nicht dürften, wollte der Beschwerdeführer wissen, wer den Firmen wirksam untersagt, personenbezogene Daten von Kunden zu erheben.

Der TLfDI bat das Unternehmen für Gebäudeservice um eine Stellungnahme zum vorgetragenen Sachverhalt. Dabei wies der TLfDI das Unternehmen darauf hin, dass nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) personenbezogene Daten aus dem Ausweis oder mithilfe des Ausweises durch öffentliche und nicht-öffentliche Stellen ausschließlich nach Maßgabe der §§ 18 bis 20 PAuswG erhoben oder verwendet werden dürfen. In der Gesetzesbegründung zu § 14 PAuswG heißt es: „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die vorgesehenen Wege erfolgen darf. (...) Weitere Verfahren z. B. über die opto-elektronische Erfassung („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“ (Drucksache des Bundesrats Nr. 550/08, S. 69 f.)

Daraus ergibt sich, dass zu Identifikationszwecken grundsätzlich nur die Stammdaten überprüft werden dürfen wie Name, Anschrift und ggf. Geburtsdatum. Daten, die nicht zur Identifizierung benötigt werden, dürfen nicht erhoben werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Kopien dürfen also nicht angefertigt werden. Lediglich die Vorlage und das anschließende Abschreiben des Namens und der Anschrift sind gesetzlich zulässig. Anschließend ist der Personalausweis dem Besitzer zurückzugeben.

Das Unternehmen teilte dem TLfDI daraufhin mit, dass aufgrund der dargelegten gesetzlichen Vorschriften in Zukunft keinerlei Kopien von Ausweisdokumenten mehr abverlangt oder weitere Angaben außerhalb der Stammdaten erhoben werden. Außerdem bestätigte das Unternehmen, seit November 2016 keine Mieterselbstauskunft von möglichen Mietinteressenten mehr abzuverlangen. Nach einer Besichtigung des Mietobjekts vermittelt die Firma nur noch den Kontakt zwischen dem Vermieter und dem Mietinteressenten. Abschließend teilte die Firma dem TLfDI im Januar 2017 mit, dass die bisher gefertigten Kopien von Ausweisdokumenten datenschutzgerecht vernichtet wurden.

Der TLfDI informierte den Beschwerdeführer über die vorgetragenen Änderungen des Serviceunternehmens und über die künftige datenschutzkonforme Mietvermittlung.

Zum damaligen Zeitpunkt war das Kopieren von Ausweisen in der Regel unzulässig. Ausnahmen galten nur für Unternehmen, die eine besondere, ausdrücklich gesetzlich geregelte „Kopiererlaubnis“ haben (beispielsweise Banken aus dem Geldwäschegesetz). Im Rahmen einer Selbstauskunft zur Anmietung von Wohnungen oder Pkw-Stellplätzen war das vermittelnde Unternehmen nicht berechtigt, Kopien von Ausweisdokumenten anzufertigen oder einzufordern.

Inzwischen hat der Gesetzgeber das Personalausweisgesetz geändert. Der Ausweis kann nunmehr seit 18. Juli 2017 nach Maßgabe des § 20 Abs. 2 PAuswG abgelichtet werden. Allerdings stellt die Norm keinen generellen Erlaubnistatbestand i. S. d. § 4 Abs. 1 BDSG dar. Die Vorschriften des Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben gemäß § 20 Abs. 2 PAuswG unberührt.

Das bedeutet, er darf nur vom Ausweisinhaber oder von anderen Personen mit dessen/deren Zustimmung abgelichtet werden und die

Ablichtung muss eindeutig als Kopie gekennzeichnet werden. Ebenfalls dürfen nur die Daten erhoben werden, mit denen der Ausweisinhaber einverstanden ist. Auch dürfen derart erstellte Kopien nicht an Dritte weitergegeben werden.

Aufgrund der Tatsache, dass die gesamte Datenverarbeitung einwilligungsbasiert ist, müssen die Kopien und die damit erhobenen Daten allerdings vernichtet werden, sobald die Einwilligung vom Ausweisinhaber widerrufen wird.

3.13 Bestattungskosten: Datenschutz kein Kostenschutz

Im Berichtszeitraum beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Bestattungsunternehmen. Das Unternehmen hatte dem Beschwerdeführer eine Rechnung zugestellt. Daraufhin bat der Beschwerdeführer das Bestattungsunternehmen um Mitteilung, woher seine Anschrift und seine Familienbeziehung zum Verstorbenen bekannt seien. Jedoch habe das Unternehmen seine Anfrage nicht beantwortet. Daher bat der Beschwerdeführer für sein Auskunftsersuchen den TLfDI um entsprechende Unterstützung.

Gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Bestattungsunternehmen verpflichtet, die vom Beschwerdeführer erbetenen Auskünfte zu erteilen. Dementsprechend bat der TLfDI das Bestattungsunternehmen um eine Stellungnahme zur nicht erteilten Auskunft.

Zwischenzeitlich hatte das Unternehmen den Beschwerdeführer jedoch schriftlich über die Herkunft seiner genutzten Daten informiert. Das Bestattungsunternehmen hatte die Daten von der Schwester des Beschwerdeführers erhalten und sicherte zu, die Daten nur zum Zwecke der Rechnungslegung verwendet und an keine andere Stelle weitergeleitet zu haben. Weiterhin bestätigte das Unternehmen schriftlich, dass die Daten nicht gespeichert würden.

Die schriftlich erteilte Auskunft des Bestattungsunternehmens genügte vollständig den Anforderungen des § 34 Abs. 1 BDSG und war somit vom TLfDI datenschutzrechtlich nicht zu beanstanden. Dies teilte der TLfDI abschließend auch dem Beschwerdeführer mit. „Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen.“ (§ 2 Abs. 4 S. 1 BDSG).

Wenn solche Stellen für sich personenbezogene Daten erheben, verarbeiten oder nutzen, sind sie „verantwortliche Stellen“ im Sinne des § 3 Abs. 7 BDSG.

Diese verantwortlichen Stellen haben dem Betroffenen auf Verlangen Auskunft zu erteilen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden, und
- den Zweck der Speicherung. (§ 34 Abs. 1 BDSG)

Die Pflicht zur Auskunftserteilung besteht insofern für jedes Unternehmen, wenn es eine entsprechende Anfrage erhält.

3.14 Unzulässige Kopie des Personalausweises – keine Bombe- nidee

Im Berichtszeitraum beschwerte sich ein Bürger über ein Unternehmen, welches Zubehör für Schwimmbäder und Saunas vertrieb. Das Unternehmen fertigte Ausweiskopien aller Kunden, die einen bestimmten Artikel kauften. Mündlich wurde dem Kunden mitgeteilt, dass dies geschehe, da der Artikel Bestandteile enthält, welche zum Bombenbauen geeignet seien. Der Bitte des Kunden, die Kopie des Personalausweises zurückzubekommen und eine schriftliche Berechtigung zur Fertigung einer solchen Kopie vorzuzeigen, kam das Unternehmen nicht nach. Des Weiteren teilte der Bürger mit, dass die Rechnungen in einem Ordner auf dem Verkaufstresen – scheinbar für jedermann zugänglich – aufbewahrt werden würden.

Der TLfDI hakte deshalb nach und bat das Unternehmen um Stellungnahme. Insbesondere wollte der TLfDI wissen, aufgrund welcher Rechtsvorschrift und in welchen Fällen die Anfertigung von Kopien des Personalausweises der Kunden erfolgt, zu welchem Zweck die Kopien erhoben werden, auf welchem Medium diese Dokumente gespeichert werden, welcher Personenkreis Zugriff auf diese Dokumente hat, wo und wie lange die Personalausweiskopien aufbewahrt werden sowie die Erläuterung zum Löschvorgang dieser Dokumente. Das Unternehmen bestätigte die Fertigung der Ausweiskopien. Diese Pflicht – so das Unternehmen dem Käufer gegenüber – ergebe sich aus den Vorgaben der Lieferanten. Denn diese fordern für dieses Produkt ein entsprechendes Chemieabgabebuch mit ge-

nauer Dokumentation. Das bedeutet, von jedem Kunden, der flüssige Produkte zur Pooldesinfektion kaufte, welche auf Aktivsauerstoffbasis mit einer Konzentration von mehr als 12 Prozent Wasserstoffperoxid versehen waren, wurde eine Kopie des Ausweises gefertigt. Grund hierfür war ein verhinderter Anschlag mit Bomben. Das Unternehmen berichtete, dass aus dem Produkt zur Pooldesinfektion das Wasserstoffperoxid gewonnen worden war, um daraus Bomben zu bauen.

Da es dem Unternehmen im Tagesgeschäft zeitlich nicht möglich war, die Daten handschriftlich zu erfassen, wurden diese Kopien gefertigt und der jeweiligen Rechnungskopie beigelegt. Somit hatte das Unternehmen einen Nachweis. Gerade auch im Hinblick auf mögliche Anschläge könnte somit – so das Unternehmen – ein gewisser Personenkreis anhand dieser Daten ermittelt werden. Kurz darauf teilte das Unternehmen mit, dass im Zuge einer Schulung festgestellt wurde, dass die Ausweiskopien nicht rechtskonform seien.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsnorm dies erlaubt oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG.

Nach § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Eine solche Erforderlichkeit zum Kopieren des Ausweises ist bei den üblichen Bargeschäften in der Regel nicht gegeben.

Die Feststellung der Identität wird nach § 3 Abs. 1 Satz 4 der Chemikalien-Verbotsverordnung (ChemVerbotsV) in diesem Fall angeordnet. Danach hatte der Verkäufer ein Abgabebuch zu führen, welches den Namen und die Anschrift des Erwerbers beinhalten musste. Allerdings war das Kopieren des Personalausweises dennoch unzulässig. Das Abgabebuch war vom Verkäufer mindestens fünf Jahre nach der letzten Eintragung aufzubewahren. Nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) durfte die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich nach Maßgabe der §§ 18 bis 20 PAuswG er-

folgen. Nach § 20 Abs. 2 PAuswG durfte dieser jenseits des elektronischen Identitätsnachweises weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Hierunter zählte auch das Kopierverfahren.

(Nach Abschluss des Verfahrens haben sich die Regelungen im PAuswG geändert. Nunmehr sind Kopien von Personalausweisen zulässig, soweit der Inhaber in die Kopie einwilligt. Allerdings darf der Inhaber selbst bestimmen, welche Daten kopiert werden dürfen und die Kopie darf nicht an Dritte weitergegeben werden.)

Der Verkäufer stellte auf Forderung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfertigung der Personalausweiskopien ein. Vielmehr wurden jetzt nur noch der Name und die Anschrift des Endkunden nach Vorlage des Personalausweises erhoben. Das zu führende Abgabebuch über das streitgegenständliche Produkt wurde in einem Stahlschrank des zusätzlich mit Alarmanlage und Sicherheitsdienst bewachten Gebäudes eingeschlossen, sodass sich niemand Zugang zu diesen sensiblen Daten verschaffen konnte.

Auch wenn eine gesetzliche Grundlage gegeben ist, personenbezogene Daten der Kunden zu erheben und zu verarbeiten, muss sich der Unternehmer auf das gesetzlich vorgegebene Maß beschränken. Zu Identifikationszwecken dürfen nach § 20 Abs. 2 PAuswG nur die hierfür erforderlichen Daten erhoben und mit dem Personalausweis abgeglichen werden.

Das Unternehmen zeigte sich sehr einsichtig im Hinblick auf datenschutzrechtliche Aspekte. Es informierte darüber, dass die Angaben, die zur Identifikation einer Person benötigt werden (Name und Anschrift), nach Vorlage des Personalausweises händisch auf der Rechnung zu dem speziellen Produkt erfasst werden können. Diese Rechnungen werden nunmehr in einem abgeschlossenen Aktenschrank aufbewahrt. Dieser ist vor unbefugtem Zugriff geschützt. Auch das Programm, mit dem die Rechnungen für die oben beschriebenen Produkte erstellt werden, ist nur nach Passworteingabe für einen bestimmten Personenkreis einsehbar. Außerdem ist das gesamte Gebäude außerhalb der Öffnungszeiten durch Alarmanlagen und Wachschatz gesichert.

Das Unternehmen hat auf Forderung des TLfDI die Arbeitsprozesse datenschutzgerecht ausgestaltet.

Zu Identifikationszwecken dürfen nach § 20 Abs. 2 PAuswG nur die hierfür erforderlichen Daten erhoben und mit dem Personalausweis abgeglichen werden. Kopien des Personalausweises sind ohne ausdrückliche Befugnis unzulässig.

3.15 Ver(un)sicherung

Dass in dem Wort „Versicherung“ zwar das Wort „sicher“ enthalten ist, seine Daten aber alles andere als das bei dieser Versicherung gewesen sind, musste ein thüringischer Bürger feststellen, als er unaufgefordert ein personalisiertes und mit seinen Daten versehenes Angebot für eine Kfz-Police von einer ihm bis dahin unbekannten Versicherung erhalten hat. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm sich der Beschwerde an und forderte die Versicherung auf, dem Beschwerdeführer eine Auskunft gemäß § 34 Bundesdatenschutzgesetz (BDSG) zu erteilen, welche Daten über ihn gespeichert wurden, woher diese Daten stammen und an wen die Daten weitergegeben worden sind. Daraufhin wurde seitens des Versicherungsunternehmens, welches sich aus dem Briefkopf des Angebots ergeben hat, mitgeteilt, dass keine Daten über den Beschwerdeführer dort hinterlegt seien und der für dieses Unternehmen vor Ort zuständige Versicherungsvertreter die Daten wohl aus seiner Erinnerung heraus in das Angebot eingefügt hätte. Nach Vorhalt des TLfDI, dass es wohl nicht der Lebenserfahrung entspreche, dass ein Versicherungsvertreter spezifische Daten wie das Erstzulassungsdatum, das Kfz-Kennzeichen, die gefahrenen Kilometer, den genauen Fahrzeugtyp usw. einfach aus der Erinnerung heraus replizieren könne, wurde weiter erklärt, dass die selbstständigen Versicherungsvertreter vor Ort die Kundendaten für sich erheben und dort möglicherweise weiter nachzufragen sei. Daraufhin wandte sich der TLfDI an den aus dem Angebot ersichtlichen Versicherungsvertreter persönlich. Dieser gab an, dass er die personenbezogenen Daten des Beschwerdeführers aufgrund seiner vorherigen Tätigkeit für eine andere Versicherung noch in seinen Unterlagen gefunden und dann für die Erstellung des Angebotes verwendet hatte.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Eine

Einwilligung des Beschwerdeführers zur Erhebung seiner Daten lag hier nicht vor, im Gegenteil, der Beschwerdeführer hatte der Verwendung der Daten auch zu Werbezwecken ausdrücklich widersprochen. Auch eine gesetzliche Erlaubnisnorm ist hier nicht gegeben. Der Versicherungsvertreter war nach § 28 Abs. 1 Nr. 1 BDSG weder dazu ermächtigt, die Kundendaten der vorherigen Versicherung zu erheben noch diese zu verarbeiten. Er hatte in diesem Fall die Kundendaten des Beschwerdeführers bei dessen Versicherung nicht für den Zweck der Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses dieses Versicherungsunternehmens erhoben, sondern für eine andere Verwendung, nämlich um diese später für Zwecke der Werbung für ein anderes Versicherungsunternehmen zu verarbeiten. Eine Erhebung dieser Daten war nach § 28 Abs. 1 Nr. 1 BDSG schon gar nicht erforderlich, da es sich nicht um eine Erhebung für eigene Geschäftszwecke gehandelt hat und eine Verwendung der erhobenen Daten zu einem anderen Zweck nach § 28 Abs. 2 Nr. 1 BDSG hier ebenfalls nicht in Betracht kam, da die Daten auch nicht allgemein zugänglich gewesen sind oder zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich waren. Mindestens überwog jedoch das schutzwürdige Interesse der betroffenen Versicherten am Ausschluss der Verarbeitung, da es dem Betroffenen obliegt, sich seine Geschäftspartner selbst auszusuchen und darüber zu bestimmen, welcher Versicherung er sein Vertrauen schenkt. Auch eine Verarbeitung und Nutzung dieser Daten zum Zwecke der Werbung nach § 28 Abs. 3 BDSG ist unzulässig, da es hier, wie oben bereits festgestellt, an einer Einwilligung des Betroffenen offensichtlich gefehlt hat.

Der selbstständige Versicherungsvertreter wurde daher durch den TLfDI aufgefordert die unzulässig erhobenen und verwendeten Kundendaten gem. § 3 Abs. 4 Nr. 5 BDSG zu löschen. Dieser Forderung kam er dann auch nach, sodass ein anordnender Bescheid in der Sache nicht mehr ergehen musste.

Wie vorliegend geschildert, gibt es immer wieder Fälle, in denen personenbezogene Daten oder ganze Datensätze, wie hier aus Versicherungsverträgen, auf unzulässige Art und Weise erhoben und zweckentfremdet werden. Diese Verwendung darf jedoch nur dann geschehen, wenn der Betroffene eingewilligt hat oder aber ein Gesetz oder eine Rechtsvorschrift dies erlaubt.

3.16 Einmal hin, einmal her – Versicherungsvermittlung ist manchmal schwer

Wie bereits im Beitrag Nummer 8.11 des 2. Tätigkeitsberichts zum Datenschutz: nicht-öffentlicher Bereich 2014/2015 berichtet, erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Versicherungskunden. Er meldete, dass sein ehemaliger Versicherungsmakler seine Kundendaten missbräuchlich verwendet hätte. Der Versicherungsmakler hatte seine Tätigkeit beim Vermittlungsbüro A aufgegeben und alle von ihm betreuten Kunden angeschrieben, um sie über seinen Wechsel zu Vermittlungsbüro B zu informieren. Im gleichen Schritt hatte er für eine Weiterführung seiner Betreuung mit dem neuen Vermittlungsbüro geworben und hierfür um eine Unterschrift auf der beigelegten Einverständniserklärung gebeten, die ihn dazu berechtigte, alle Versicherungspolicen auf das neue Vermittlungsbüro B umzustellen.

Der Beschwerdeführer unterschrieb solch eine zunächst, widerrief die Einwilligung aber wieder nach sechs Tagen.

Nach § 4 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Umstellung der Versicherungspolicen erfolgte zunächst aufgrund der Einwilligung durch den Beschwerdeführer. Mit Einlegen des Widerrufs erlosch diese jedoch. Daraufhin stoppte der Versicherungsmakler die bereits vorgenommenen Schritte in der Umstellung. Das Versicherungsunternehmen wurde benachrichtigt, die Policen wieder auf das Vermittlungsbüro A zu übertragen. Somit wäre der Vorgang eigentlich erledigt gewesen.

Allerdings meldete sich der Beschwerdeführer nach einiger Zeit erneut beim TLfDI. Ihm wurde vom Versicherungsunternehmen abermals mitgeteilt, dass seine Versicherungspolicen, entgegen seinem Widerruf, über das Vermittlungsbüro B laufen. Der TLfDI wandte sich dann mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an den Versicherungsmakler und das Versicherungsunternehmen, für das er tätig gewesen ist. Dabei stellte sich jedoch heraus, dass dem Versicherungsunternehmen bei der Verarbeitung ein Fehler unterlaufen war. Die notwendigen Änderungen im Vertrag haben sich ungünstig überschneiden, sodass die ursprünglich gewollte

Rückabwicklung nicht veranlasst wurde. Nachdem dieser Fehler aufgrund der Rückfrage des TLfDI aufgedeckt worden war, wurden die Versicherungspolizen so wie anfänglich veranlasst wieder zum Vermittlungsbüro A rückabgewickelt.

Gem. § 4 BDSG ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Sobald eine Einwilligung widerrufen wird, ist für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die nur aufgrund einer Einwilligung des Betroffenen vorstattengehen, keine Ermächtigung mehr vorhanden. Die weitere Verwendung der personenbezogenen Daten muss sofort eingestellt werden. Außerdem sind die Daten, falls keine Aufbewahrungsfristen dagegen sprechen, unwiderruflich zu löschen.

3.17 Seminararbeit im Netz: nur ohne Personenbezug

Aufgrund einer Beschwerde wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass auf der Website eines Unternehmens eine Seminararbeit ohne Einwilligung der in der Seminararbeit erwähnten Personen veröffentlicht wurde. Darin waren auch personenbezogene Daten des Beschwerdeführers, der die Seminararbeit unterstützte, enthalten. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Es reicht also aus, wenn die Person noch bestimmbar ist. Nur durch Weglassen des Namens in einem Datensatz oder Dokument fehlt es nicht an der Bestimmbarkeit, wenn die äußeren Umstände eine Identifizierung zulassen. Im Fall der Seminararbeit traf dies zu, da diese über eine bestimmte Stelle berichtete und aufgrund der dortigen beruflichen Tätigkeit des Beschwerdeführers ein Bezug zum Beschwerdeführer unschwer hergestellt werden konnte. Mittels Auskunftersuchen wurde das verantwortliche Unternehmen angeschrieben. Die Website mit der veröffentlichten Seminararbeit wurde daraufhin offline gestellt und das Dokument stillgelegt.

Das Verarbeiten von personenbezogenen Daten ist gem. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) zulässig, wenn dies durch das BDSG oder eine andere Rechtsvorschrift erlaubt ist oder angeordnet

wird oder der Betroffene in die Verarbeitung eingewilligt hat. Unter den Begriff der personenbezogenen Daten fallen auch solche Informationen, die einer Person mittelbar zugeordnet werden können und damit auch die vorliegende Seminararbeit.

Aufgrund der Veröffentlichung der personenbezogenen Daten auf der Website des Unternehmens wurden diese einer unbestimmten Anzahl von Dritten zur Verfügung gestellt und somit verarbeitet. Unter Verarbeiten fällt gemäß § 3 Abs. 4 BDSG das Übermitteln personenbezogener Daten. Übermitteln bedeutet nach § 3 Abs. 4 Nr. 3a) BDSG wiederum das Bekanntgeben von Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden. Eine Rechtsvorschrift im BDSG oder anderen Gesetzen, die die Veröffentlichung der Daten erlaubt oder anordnet, war vorliegend nicht gegeben. In diesem Fall wäre eine Einwilligung der Betroffenen zur Veröffentlichung der Seminararbeit erforderlich gewesen, welche aber nicht erteilt wurde. Die Datenverarbeitung war daher unzulässig. Aufgrund des Tätigwerdens des TLfDI konnten durch das Offlinestellen der Website mit deren sämtlichen Inhalten datenschutzkonforme Zustände wiederhergestellt werden, sodass der Beschwerdeführer in seinem Recht auf informationelle Selbstbestimmung nicht mehr verletzt war.

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Es reicht also aus, wenn die Person noch bestimmbar ist. Im vorliegenden Fall erfolgte zwar keine namentliche Nennung, jedoch konnte durch die Informationen, die in der Arbeit enthalten waren, die betreffende Person ohne großen Aufwand identifiziert werden.

3.18 Welche Mitgliederdaten darf ein Verein erheben und an seinen Dachverband weitergeben?

Im November 2016 bat der Thüringer Landesverband eines Vereins den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die Information, ob seine Satzung hinsichtlich der datenschutzrechtlichen Bestimmungen angepasst werden muss. Hierbei ging es insbesondere darum, welche Mitgliederdaten der Landesverband erheben, verarbeiten und an seine Dachverbände weitergeben darf und welche datenschutzrechtlichen

Informationen auf den Mitgliedsanträgen des Verbands aufgeführt werden müssen. Weiterhin wollte der Landesverband wissen, ob Datenschutzerklärungen für Amtsträger und hauptamtliche Mitarbeiter im Kreis-, Landes-, Bundes- und Europaverband notwendig sind. Der TLfDI legte dar, dass er nicht die zuständige Aufsichtsbehörde für den Bundes- und den Europaverband des Vereins ist. Zuständige Aufsichtsbehörde für den Bundesverband mit Sitz in Berlin sei der Berliner Datenschutzbeauftragte und für den Europaverband die Commission de la protection de la vie privée in Brüssel. Dementsprechend bot der TLfDI an, die Anfrage des Landesverbandes an die zuständigen Stellen weiterzuleiten.

In Bezug auf den Landesverband Thüringen beantwortete der TLfDI die Fragen des Verbandes folgendermaßen: Vereine, die personenbezogene Daten erheben und verarbeiten, sind gemäß § 2 Abs. 4 Satz 1 Bundesdatenschutzgesetz (BDSG) nicht-öffentliche Stellen, auf die das BDSG Anwendung findet (§ 1 Abs. 2 Nr. 3 BDSG).

Nach § 4 Abs. 1 BDSG dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die betroffene Person eingewilligt hat. Eine Vereinssatzung kann jedoch, ebenso wenig wie die Satzung eines Dachverbands, als Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG das Schutzniveau des BDSG unterschreiten. Daher bedarf es einer anderen Rechtsnorm. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten – im vorliegenden Falle Mitgliederdaten – oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist. Einem Schuldverhältnis immanent sind gegenseitige Rechte und Pflichten.

Die Mitgliedschaft in einem Verein bzw. dessen Landesverband ist als ein Schuldverhältnis im Sinne des § 28 Abs. 1 Satz 1 Nr. 1 BDSG anzusehen. Denn hier bestehen Rechte und Pflichten der Mitglieder untereinander und zum Verein. Diese Rechte und Pflichten ergeben sich überwiegend aus dem Inhalt der Vereinssatzung. Der durch die Satzung verfolgte Vereinszweck ist gem. § 28 Abs. 1 Nr. 1 BDSG maßgebend für die Zulässigkeit der Datenverarbeitung. Daher darf der Landesverband Thüringen nur die Daten seiner Mitglieder erheben, die er zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt. Daher ist für den

Umgang mit den Mitgliedsdaten regelmäßig § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebende Rechtsgrundlage. Somit darf der Landesverband auf seinen Mitglieds- bzw. Aufnahmeanträgen beim Beitritt eines Mitglieds gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur die personenbezogenen Daten erheben, die für die Begründung und Durchführung des Mitgliedsverhältnisses benötigt werden. Die dafür erforderlichen Daten müssen im Mitgliedsantrag festgelegt und entsprechend gekennzeichnet werden.

Um seinen Vereinszweck erfüllen zu können, benötigt der Thüringer Landesverband in jedem Falle die „Korrespondenzdaten“ (Name und Anschrift) seiner Mitglieder. Sofern weitere Daten für die Vereinsarbeit erforderlich sind, dürfen auch diese erhoben werden (Beispiel: Kontodaten für den Lastschrifteinzug des Mitgliedsbeitrags). Letztlich muss aber immer gewährleistet sein, dass die Vereinsmitglieder hierüber informiert werden. Nach § 4 Abs. 3 BDSG ist der Betroffene über folgende Umstände in Kenntnis zu setzen:

1. die Identität der verantwortlichen Stelle (der Landesverband Thüringen),
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung der Daten,
3. die Empfänger der Daten, soweit die Daten weitergeleitet werden und der Betroffene nicht mit einer Übermittlung zu rechnen hatte.

Für nicht erforderliche Daten zur Begründung und Durchführung des Vereinsverhältnisses muss es dem jeweiligen Mitglied selbst überlassen bleiben, ob es Angaben dazu machen möchte oder nicht. Nach der Satzung des Landesverbandes können natürliche Personen, die das 35. Lebensjahr noch nicht vollendet haben, ordentliche Mitglieder werden. Somit ist auch die Angabe des Geburtsdatums für die Mitgliedschaft wichtig. Die Pflichtangabe der E-Mail-Adresse der Mitglieder in der Satzung des Landesverbandes ist nicht zulässig, weil es jedem Mitglied selbst überlassen bleiben muss, ob es diesen Weg der Kommunikation zulassen möchte oder nicht.

Bei der Frage, welche Mitgliederdaten erforderlich sind, muss immer der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a Satz 1 BDSG beachtet werden. In diesem Sinne sollte auch die Angabe der Telefonnummer dem Mitglied freigestellt werden, da dies zur Verfolgung der Vereinsziele sowie für die Betreuung und Verwaltung der Mitglieder nicht erforderlich erscheint. Insofern

sollte diese Angabe ausdrücklich als „Freiwillige Angabe“ im Aufnahmeantrag aufgeführt werden.

Nach Ansicht des TLfDI ist es empfehlenswert, von jedem Mitglied schon beim Eintritt in den Verein eine Einwilligungserklärung nach BDSG einzuholen. Diese Einwilligung sollte sich optisch vom Beitrittsformular unterscheiden und mit einer gesonderten Unterschrift bestätigt werden. Im Mitgliedsantrag wird die Einwilligung nach BDSG zusammen mit den anderen Erklärungen zur Mitgliedschaft schriftlich erteilt. Insofern schlug der TLfDI vor, dies im Sinne von § 4a Abs. 1 BDSG drucktechnisch besonders (z. B. farbig) kenntlich zu machen.

Soweit der Landesverband Thüringen seine Mitgliederdaten an die Dachverbände (Bundes- und Europaverband) weitergibt, handelt es sich um eine Datenübermittlung an Dritte im Sinne des § 3 Abs. 4 Nr. 3 BDSG, da gemäß § 3 Abs. 8 Satz 2 BDSG ein Bundes- oder Europaverband im Verhältnis zum Landesverband ein sogenannter Dritter ist. Somit benötigt der Landesverband, wenn er seine Mitgliedsdaten an den Bundes- oder Europaverband übermitteln will, eine Rechtsgrundlage oder die ausdrückliche Einwilligung der betroffenen Mitglieder. Dies ist nur dann unproblematisch, wenn es lediglich um die Übermittlung von anonymisierten Daten zu statistischen Zwecken geht, beispielsweise die Anzahl der Mitglieder, da dann überhaupt keine personenbezogenen Daten verarbeitet werden.

Nach Kenntnis des TLfDI und aufgrund seiner Satzung ist der Landesverband Thüringen jedoch dazu verpflichtet, die in der Satzung benannten konkreten personenbezogenen Daten seiner Mitglieder (Name, Geschlecht, Geburtsdatum, Anschrift, Telefonnummer und E-Mail-Adresse) an den Bundesverband weiterzugeben. Dort werden diese Daten im Rahmen der Mitgliedschaft für interne Vereinszwecke verarbeitet und genutzt, insbesondere für die Mitgliederverwaltung, -information und -betreuung. Für die Weitergabe der Daten an die Dachverbände empfahl der TLfDI dem Landesverband Thüringen, entsprechende klare Regelungen bereits beim Eintritt in den Landesverband festzuschreiben und eindeutig im Mitgliedsantrag zu formulieren. Diese Satzungsklauseln sind verbindlich für alle Vereinsmitglieder, da sie den Regelungen durch ihre Mitgliedschaft und die damit verbundene Anerkennung der Satzung zustimmen und insofern zur genannten Verwendung der Daten eine persönliche Einwilligung erteilen.

Die Frage des Landesverbandes, ob Datenschutzerklärungen für Amtsträger und hauptamtliche Mitarbeiter im Kreis-, Landes-, Bundes- und Europaverband notwendig sind, beantwortete der TLfDI folgendermaßen: Personen, die mit der Verarbeitung von personenbezogenen Daten betraut sind, müssen gemäß § 5 BDSG auf das Datengeheimnis verpflichtet werden. Dies gilt auch für ehrenamtlich im Verein tätige Personen, wenn sie mit der Datenverarbeitung befasst sind. Dazu sollte der Landesverband ein Merkblatt vorbereiten und per Unterschrift von den betreffenden Personen bestätigen lassen. Der TLfDI verwies hierzu auf die Mustervorlage zur Verpflichtung auf das Datenschutzgeheimnis auf seiner Internetseite unter <https://www.tlfdi.de/tlfdi/themen/unternehmen/>. Diese Vorlage müsste der Thüringer Landesverband ggf. an seine Bedürfnisse anpassen.



Vereine, die personenbezogene Daten erheben und verarbeiten sind gemäß § 2 Abs. 4 Satz 1 Bundesdatenschutzgesetz (BDSG) nicht-öffentliche Stellen, auf die das BDSG anzuwenden ist (§ 1 Abs. 2 Nr. 3 BDSG). Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist. Ein Schuldverhältnis ist eine Rechtsbeziehung mit gegenseitigen Rechten und Pflichten. Im Rahmen der Vereins- oder Verbandsmitgliedschaft bestehen Rechte und Pflichten der Mitglieder untereinander und zum Verein.

Bei der Frage, welche Mitgliederdaten erforderlich sind, muss immer der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a Satz 1 BDSG beachtet werden. Die E-Mail-Adresse und die Telefonnummer zählen nicht zu den zwingend erforderlichen (Korrespondenz-)Daten zur Erfüllung der Vereinszwecke. Dies sind vorrangig Name und Anschrift des Vereinsmitglieds und – sofern die Vereinssatzung eine Altersgrenze für die Mitgliedschaft vorschreibt – das Geburtsjahr.

Für die Weitergabe seiner Mitgliederdaten an einen übergeordneten oder Dachverband benötigt der Verein eine Rechtsgrundlage oder die

ausdrückliche Einwilligung der betroffenen Mitglieder. Der TLfDI empfiehlt, von jedem Mitglied schon beim Eintritt in den Verein eine Einwilligungserklärung nach BDSG einzuholen

3.19 Zahlartensteuerung – nein, danke!

Der Onlinehandel ist für den Kunden eine bequeme und schnelle Art des Einkaufens. Er hat eine nahezu unendlich große Auswahl an Produkten und entscheidet sich dann für das attraktivste Angebot. Dass dies aber leider nicht für die Abwicklung des Kaufes und die Auswahl der bevorzugten Zahlart zutrifft, musste ein Betroffener feststellen, als er in einem Thüringer Online-Versandhandel seinen Warenkorb füllte und dann per Kreditkarte zahlen wollte. Der Betroffene hatte seine persönlichen Daten, wie Name, Adresse, Geburtsdatum usw., eingegeben und wurde dann zur Zahlartenauswahl weitergeleitet, wo ihm dann aber nur der Kauf per Vorkasse oder Sofortüberweisung angeboten wurde, obwohl das Unternehmen auch andere Zahlarten, wie Kauf auf Rechnung, Kreditkarte, Lastschrift oder PayPal, anbietet. Verwundert über diese doch sehr geringe Auswahlmöglichkeit in seinem Fall, wandte sich der Betroffene an das Unternehmen und erhielt dort die Auskunft, dass im Vorfeld der Zahlartenauswahl, eine Bonitätsabfrage bei einer Wirtschaftsauskunftei veranlasst wird und entsprechend dem Ergebnis dieser Abfrage für ihn nur begrenzte Zahlarten zur Verfügung stehen. Der Betroffene sah darin einen Verstoß gegen datenschutzrechtliche Vorgaben und wandte sich mit der Bitte um Prüfung dieses Vorgehens bei der Bestellung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Datenschutzaufsicht für in Thüringen ansässige Unternehmen.

Der TLfDI forderte daher das Unternehmen zur Auskunft darüber auf, inwieweit das vom Betroffenen geschilderte Prozedere zutrifft und wann genau die Abfrage bei der Wirtschaftsauskunftei erfolgt. Der TLfDI vertrat dabei die Auffassung, dass die Abfrage bei der Wirtschaftskanzlei noch vor Eingabe der Zahlart ein unzulässiges Vorgehen darstellt. Dabei ist ausschlaggebend, dass die Zulässigkeit der Datenverarbeitung sich aufgrund des Bundesdatenschutzgesetzes (BDSG) oder einer anderen Rechtsvorschrift ergeben muss. Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, soweit es zur Wahrung berechtigter Inte-

ressen der verantwortlichen Stelle dient und erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG).

Ein berechtigtes Interesse des Unternehmens daran, das kreditorische Risiko bei unsicheren Zahlarten gering zu halten, ist durchaus als gegeben anzunehmen. Eine Zahlartensteuerung ist aber zur Wahrung dieses Interesses keinesfalls erforderlich. Es reicht nicht aus, dass aus der Sicht des Unternehmens die Verwendung geeignet oder zweckmäßig erscheint. Im Bestellprozess des Unternehmens wurde noch vor der Entscheidung des Kunden für eine bestimmte, möglicherweise ein kreditorisches Risiko auslösende Zahlart eine Bonitätsprüfung bei einer Auskunft einverlangt. Die Bonitätsabfrage wurde damit auf einen Zeitpunkt vorverlagert, zu dem sie noch überhaupt nicht für die Wahrung des berechtigten Interesses des Unternehmens erforderlich war.

Es ist dem Onlinehändler ohne weiteres möglich, eine Auswahl der vom Kunden beabsichtigten Zahlart abzuwarten und erst bei Entscheidung für eine unsichere Zahlmethode eine Bonitätsauskunft bei einer Auskunft einzuholen. Die Auswahlmöglichkeit des Kunden muss sich auf alle angebotenen Zahlarten beziehen. Die für den Betreiber unsicheren Zahlmethoden (Rechnung und Lastschrift) sind zudem mit dem Hinweis zu versehen, dass bei Auswahl ggf. eine Bonitätsprüfung vorbehalten bleibt. Insoweit wird auch dem Transparenzgebot Rechnung getragen und der Kunde vorab darüber informiert, mit welchen Konsequenzen er bei Auswahl einer bestimmten Zahlart rechnen muss.

Die Abfrage bei einer Auskunft darf erst dann erfolgen, wenn der Kunde sich im Rahmen des Bestellvorgangs für eine bestimmte Zahlart entschieden hat. Für den Fall der Entscheidung für eine sog. risikolose Zahlart (Vorkasse, Kreditkarte, paypal u. ä.), also solche, bei denen für ein Unternehmen kein kreditorisches Risiko entsteht, ist eine Abfrage bei einer Auskunft keinesfalls erforderlich und verstößt damit gegen die Regelungen des BDSG. In jedem Fall aber sind die hier beschriebenen Zahlartensteuerungen unzulässig.

3.20 Der TLfDI macht viel – aber nicht alles

Besorgte Bürger wandten sich auch im aktuellen Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit gut 100 Anfragen und Beschwerden, die nicht in die Zuständigkeit des TLfDI fielen. Denn der TLfDI kontrolliert gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Die örtliche Zuständigkeit richtet sich grundsätzlich nach dem Sitz der für die Datenverarbeitung verantwortlichen Stelle bzw. nach dem Ort einer Betriebsstätte. Gingen die Beschwerden der Bürger per E-Mail ein, so wurde den Beschwerdeführern die Adresse der zuständigen Aufsichtsbehörde genannt. Gingen die Beschwerden per Briefpost beim TLfDI ein, wurde über die Nichtzuständigkeit des TLfDI informiert und angefragt, ob die Anfrage an die zuständige Stelle gesandt werden soll. Bei Einverständnis des Beschwerdeführers wurde das Schreiben weitergeleitet.

Beispiele für die Unzuständigkeit des TLfDI

Nicht zuständig ist der TLfDI z. B. für die Bereiche Telekommunikation, Rundfunk (Radio und Fernsehen), kirchliche Stellen und Jobcenter (sofern es sich nicht um Optionskommunen handelt). Welche Stellen hierfür jeweils zuständig sind, wurde bereits im 2. Tätigkeitsbericht unter 2.35 näher erläutert.

Ebenfalls nicht zuständig ist der TLfDI für die Datenschutzkontrolle von Postdienstunternehmen. Für die Kontrolle dieser Unternehmen ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit Sitz in 53117 Bonn, Husarenstraße 30, E-Mail: poststelle@bfdi.bund.de zuständig, unabhängig davon, wo der Sitz des Unternehmens ist.

Für die Kontrolle der Verarbeitung von personenbezogenen Daten bei den Krankenkassen ist das jeweilige Bundesland, in welchem der Hauptsitz ist, zuständig, auch wenn es in Thüringen eine entsprechende Niederlassung gibt.

Die Beschwerden über die Schufa müssen an den Hessischen Datenschutzbeauftragten, Gustav-Stresemann-Ring 1 in 65189 Wiesbaden gerichtet werden, da der Sitz der SCHUFA in Wiesbaden ist.



Bei Beschwerden über Unternehmen, die ihre Hauptniederlassung im Ausland haben, ist die jeweilige Datenschutzaufsichtsbehörde des Landes zuständig. Die entsprechenden Adressen und Ansprechpartner findet man im Virtuellen Datenschutzbüro unter <https://www.datenschutz.de>.

Die Zuständigkeit der Kontrolle des TLfDI richtet sich nach dem Sitz der Daten verarbeitenden Stelle bzw. nach dem Hauptsitz der Betriebsstätte. Denn der TLfDI kontrolliert gemäß § 37 ThürDSG bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 BDSG Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen.

3.21 Pressefreiheit versus Datenschutz?

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass die Presse personenbezogene Daten veröffentlichte. Der Bürger hatte sich mit Missständen innerhalb seiner Kommune an die Presse gewandt. Diese veröffentlichte hierzu auch einen Artikel, jedoch nicht nur das. Während der Bürger die Veröffentlichung begrüßte, da er damit ja auch etwas bewirken wollte, rechnete er jedoch nicht mit der Veröffentlichung seines vollständigen Namens. Er war der Überzeugung, dass dies eine erhebliche Verletzung des Datenschutzes sei und bat um diesbezügliche Klärung. Des Weiteren wollte er wissen, ob und welche rechtlichen Schritte er gegen die Zeitung einleiten kann.

Leider kann der TLfDI nur den Dingen nachgehen, die im Rahmen seiner Zuständigkeiten liegen. Dies ist im Pressebereich in der Regel nicht der Fall. So regelt § 41 BDSG das sogenannte Presseprivileg. Darin wird geregelt, dass der Landesgesetzgeber in bestimmten Bereichen Regelungen für die Presse erlassen muss. Dort regelt der Landesgesetzgeber in § 11a Thüringer Pressegesetz:

Soweit Unternehmen oder Hilfsunternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten von den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) nur die §§ 5, 9 und 38a sowie § 7 mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung des Datengeheimnisses nach § 5 BDSG oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des § 9 BDSG eintreten.

Da damit die Anwendung von § 38 BDSG bei rein redaktionellen oder journalistischen Tätigkeiten ausgeschlossen ist, sich die Zuständigkeit des TLfDI aber aus § 38 Abs. 6 BDSG (i. V. m. § 42 Abs. 1 Thüringer Datenschutzgesetz) ergibt, folgt daraus die Unzuständigkeit des TLfDI in solchen rein redaktionellen oder journalistischen Tätigkeiten.

Anwendbar bleibt das BDSG jedoch, wenn es sich nicht um eine reine redaktionelle oder journalistische Tätigkeit handelt, § 41 Abs. 1 BDSG.

Im hier vorliegenden Fall handelte es sich jedoch ganz klar um eine rein journalistische Angelegenheit, weswegen der TLfDI dem Bürger gegenüber seine Unzuständigkeit erklärt hätte.

Noch bevor der TLfDI im Fall irgendetwas unternehmen konnte, meldete sich der betroffene Bürger jedoch nochmals und teilte mit, er wünsche doch keine Verfolgung, da sich die Redaktion entschuldigt habe.

Dem Bürger wurde dennoch mitgeteilt, dass der TLfDI für die hiesige Beschwerde über den mutmaßlichen Datenschutzverstoß ohnehin nicht die zuständige Behörde sei, da es sich um eine rein journalistische Angelegenheit handelt und der TLfDI insoweit nicht Aufsichtsbehörde sei. Sollte der Bürger trotzdem eine Prüfung wünschen, müsse er sich an den Deutschen Presserat wenden.

Zwar ist der TLfDI bei rein redaktionellen oder journalistischen Tätigkeiten nicht die zuständige Aufsichtsbehörde, jedoch müssen diese Voraussetzungen auch greifen. Handelt es sich nicht um eine ausschließlich journalistische oder ausschließlich redaktionelle Tätigkeit, sondern werden die personenbezogenen Daten auch anderweitig verwendet, ist der TLfDI zuständig.

3.22 Wie oft muss man der Hausbank den Personalausweis vorlegen?

Ein Bankkunde wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er im Jahr 2016 ohne Angabe der Rechtsgrundlage von seiner Bankfiliale in Thüringen aufgefordert worden war, seinen Personalausweis zum Zweck der Aktualisierung der Ausweisdaten im System der Bank zur Filiale mitzubringen. Bereits drei Jahre zuvor war der Kunde nämlich auch schon zur Vorlage seines Personalausweises aufgefordert worden, wobei sich bei der damaligen Prüfung durch den Datenschutzbeauftragten der Bank ergab, dass hierfür keine Rechtsgrundlage bestand bzw. die angegebene Rechtsgrundlage (§ 154 Abgabenordnung) keine Vorlage des Ausweises begründete und der Bank ein Fehler unterlaufen war.

Die Datenschutzabteilung der Bank erklärte dem TLfDI auf seine Nachfrage, dass die Bank nach den §§ 3 und 4 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) im Rahmen ihrer Sorgfaltspflicht zur Identifizierung und kontinuierlichen Überwachung ihrer Vertragspartner verpflichtet sei. Gemäß § 3 Abs. 1 Nr. 4 GwG müsse daher sichergestellt werden, dass die jeweiligen Dokumente, Daten oder Informationen in angemessenem zeitlichen Abstand aktualisiert werden. Eine erneute Legitimation des Bankkunden durch Vorlage des Ausweises sei eigentlich nur dann erforderlich, wenn zum Beispiel bei der Kontoeröffnung die Dokumente nicht vollständig oder nur in Kopie vorgelegt werden konnten. Dies sei im vorliegenden Fall aber nicht gegeben gewesen, vielmehr sei aufgrund eines Versehens die erneute Legitimation erbeten worden. Dafür habe man sich beim Beschwerdeführer bereits entschuldigt.

Auch wenn der Beschwerdeführer bereits zum zweiten Mal zur Vorlage von Identifikationspapieren zur Aktualisierung aufgefordert wurde, ohne dass die konkrete Rechtsgrundlage angegeben worden war, hat der TLfDI das jeweilige Versehen zwar als unverständlich angesehen, weitere Nachforschungen waren jedoch nicht angezeigt, denn eine unzulässige Erhebung und Verarbeitung nicht erforderlicher Daten erfolgte letztendlich nicht.

Banken sind nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) im Rahmen

ihrer Sorgfaltspflicht zur Identifizierung und kontinuierlichen Überwachung ihrer Vertragspartner verpflichtet. Sie müssen sicherstellen, dass die jeweiligen Dokumente, Daten oder Informationen in angemessenem zeitlichem Abstand aktualisiert werden. Jede Aufforderung, die Ausweispapiere vorzulegen, bedarf einer Rechtsgrundlage, die gegenüber dem Betroffenen angegeben werden muss.

3.23 Wenn die Hausbank keine Auskunft erteilt

Ein Rechtsanwalt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich im Namen seines Mandanten darüber, dass von einer Bankfiliale in Thüringen seine Fragen nicht beantwortet wurden. Das Auskunftsbegehren nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) bezog sich auf die zur Person des Mandanten gespeicherten Daten, deren Herkunft sowie der Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben wurden. Hintergrund war, dass offenbar Gerüchte und Informationen über die Firma des Mandanten kursierten, deren Ursprung der Mandant in der Bank vermutete. Schließlich sah er dadurch seine Firma in Misskredit gezogen.

Der TLfDI wandte sich mit einem Auskunftsbegehren nach § 38 Abs. 1 Satz 1 BDSG an die Bankfiliale. Postwendend teilte die für Datenschutz zuständige Abteilung am Hauptsitz der überregionalen Bank mit, der TLfDI habe offensichtlich übersehen, dass sich der Sitz der nicht-öffentlichen Stelle nicht in Thüringen befinde und solle sich mit der zuständigen Datenschutzaufsichtsbehörde in Verbindung setzen. Der TLfDI wies darauf hin, dass die Zuständigkeit der Datenschutzaufsicht in Thüringen nicht als grundsätzlich ausgeschlossen angesehen werden könne. § 3 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz bestimmt nämlich die örtliche Zuständigkeit für Betriebsstätten in Thüringen, die dann beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit liegt, wenn eine Angelegenheit von der Betriebsstätte selbst vorgenommen oder geregelt wird. Die Abteilung Datenschutz der Bank am Hauptsitz legte daraufhin dar, dass eine Auskunftserteilung im Rahmen des § 34 BDSG ausschließlich durch den betrieblichen Datenschutbeauftragten am Hauptsitz der Bank erfolge. Die Filialen (Betriebsstätten) lieferten hierzu gegebenenfalls Informationen, eine eigenständige Auskunftserteilung durch die Filiale erfolge jedoch

nicht. Im Übrigen habe man die Anfrage des TLfDI bereits zum Anlass genommen, dem Kunden die gewünschte Auskunft zu erteilen. Der Anwalt des Kunden sah jedoch durch die offenbar erteilte Auskunft noch keine Erledigung der Sache und bat den TLfDI um Abgabe an die für den Hauptsitz zuständige Datenschutzaufsicht. Dem kam der TLfDI selbstverständlich nach.

Der TLfDI ist nach § 3 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz zuständige Datenschutzaufsicht für Betriebsstätten in Thüringen. Handelt es sich dabei um Niederlassungen eines überregionalen Unternehmens mit Hauptsitz in einem anderen Bundesland, ist zu prüfen, ob die Betriebsstätte oder Filiale in Thüringen eigene Handlungsspielräume oder Regelungskompetenzen hat. Wird dies verneint, ist der Vorgang an die für den Sitz des Hauptunternehmens zuständige Datenschutzaufsicht abzugeben.

3.24 Frage eines Software-Entwicklers: Veröffentlichung von Vertretungsplänen sowie Stundenplänen innerhalb einer App für Schulen

„Ist nun morgen Deutsch statt Astro in der Ersten?“ „Haben wir nachher Sport bei Herrn Freistoß oder vertritt Frau Sprint?“ – Ganz normale Fragen im Schulalltag. Die Antworten darauf ändern sich oft schneller wie der Vertretungsplan, der vor dem Lehrerzimmer hängt. Da wär’ doch eine Info auf dem Smartphone ganz sinnvoll, oder?

Die Verwendung moderner Kommunikationskanäle hat auch in vielen Schulen Einzug gehalten. Oft nutzen sie ihre Internetseiten, um Informationen an Schüler, Lehrer und Eltern schnell und papierlos zu verteilen. Dabei stellt sich oft die Frage, ob die Verteilung personenbezogener Informationen, die ja regelmäßig in solchen Nachrichten stecken, datenschutzrechtlich immer o. k. ist oder nicht.

Diese Frage sollte auch Softwarefirmen beschäftigen, die einen Bedarf an Applikationen für die Zielgruppe Schule sehen und decken wollen. Erfreulich ist es, wenn diese Sensibilität besteht. Datenschutzfreundliche Programme sind durchaus nicht die Regel, wie viele Beispiele beweisen. Dass es anders geht, beweist eine Anfrage eines Softwareherstellers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er bat um Klärung, ob Vertretungspläne in einem passwortgeschützten Bereich

zulässig wären, auf den nur Schüler der jeweiligen Schule und ggf. auch nur der betroffenen Klasse Zugriff haben. Der TLfDI antwortete, dass dies grundsätzlich möglich sei. Auch gegen die Veröffentlichung der Namen der vertretenden Lehrkräfte spräche dann nichts, wenn die Schule dies aus bestimmten Gründen für erforderlich hält. Klargestellt wurde aber auch, dass eine Veröffentlichung im jedermann zugänglichen Bereich der Schulhomepage, ggf. unter Bekanntgabe der Lehreramen, nicht zulässig wäre, weil dies zur Aufgabenerfüllung der Schule nicht erforderlich ist. Insgesamt ist es wichtig, die Datenflüsse entsprechend den Anforderungen des Datenschutzrechts zu gestalten. Sobald der Softwarefirma etwa für die Anmeldung personenbezogene Daten übermittelt werden, ist ein Vertrag über die Auftragsdatenverarbeitung zu schließen. Im Hinblick auf die grundsätzlichen Probleme der Nutzung von Apps an Schulen wird auf den Beitrag unter Punkt 12.29 im 12. Tätigkeitsbericht des TLfDI im öffentlichen Teil verwiesen.

Den TLfDI erreichte eine Anfrage, ob Vertretungspläne von Schulen inkl. Lehreramen in passwortgeschützten Bereichen von Apps erlaubt seien. Der TLfDI bestätigte das grundsätzlich, wies jedoch darauf hin, dass im Gegensatz dazu eine Veröffentlichung in für jedermann zugänglichen Bereichen von Schulhomepages o. ä. für die Aufgabenerfüllung der Schule grundsätzlich nicht erforderlich und damit unzulässig ist.

3.25 Mitgliedsbeiträge am schwarzen Brett?

Der Betriebsrat der Beschäftigten eines gemeinnützigen Vereins wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Einschätzung, ob die Geschäftsleitung befugt sei, Listen für alle Mitarbeiter einsehbar auszuhängen, aus denen ersichtlich ist, welche Mitgliedsbeiträge die einzelnen Beschäftigten bezahlen. Dabei war in der Satzung des gemeinnützigen Vereins kein Mindestbeitrag festgelegt worden, jedoch hatte man seitens der Geschäftsleitung Vorstellungen, welche Beträge entrichtet werden sollten. Auch wollte man Anreize schaffen, dass diejenigen Mitarbeiter, die noch nicht Mitglied in dem gemeinnützigen Verein waren, beitreten und ebenfalls Beiträge entrichten. Durch diese Vorgehensweise fühlten sich die Mitarbeiter unter Druck gesetzt.

Beratend führte der TLfDI aus, der Aushang der Liste stelle eine Verarbeitung von Beschäftigtendaten verschiedener Betroffener in der Form der Übermittlung an andere Mitarbeiter dar, die nur dann zulässig sei, wenn eine Rechtsgrundlage hierfür existiert. Eine solche sei jedoch nicht erkennbar. § 32 Bundesdatenschutzgesetz (BDSG) als maßgebliche Vorschrift für die Verarbeitung von Beschäftigtendaten könne hierfür nicht herangezogen werden. Selbst wenn die Vereinsmitgliedschaft im Falle eines sogenannten Tendenzbetriebs Voraussetzung für die Beschäftigten sein sollte und daher unter Umständen vom Arbeitgeber erhoben und verarbeitet werden dürfte, rechtfertigte dies noch keine Übermittlung an andere Mitarbeiter.

Auch eine Einwilligung nach § 4a Abs. 1 Satz 3 BDSG konnte keine Rechtsgrundlage für die eingangs geschilderte Vorgehensweise bilden. Maßgeblich für eine wirksame Einwilligung ist, dass sie auf Freiwilligkeit beruht, wovon im Beschäftigtenverhältnis regelmäßig nicht ausgegangen werden kann, weil der Beschäftigte möglicherweise im Falle einer Verweigerung der Einwilligung mit Nachteilen rechnet.

Im Ergebnis war die Veröffentlichung der Namen und der Mitgliedsbeiträge von Vereinen weder mit noch ohne Zustimmung der Betroffenen zulässig.

Für den Betriebsrat war die Auskunft offenbar hilfreich.

Ein gemeinnütziger Verein ist nicht befugt, die Mitgliedschaft und die entrichteten Mitgliedsbeiträge der bei ihm Beschäftigten zu veröffentlichen. Weder § 32 BDSG noch die Einwilligung der Betroffenen können eine Rechtsgrundlage hierfür bilden.

3.26 Der Übergang von Kundendaten bei Unternehmensverkäufen

Im Rahmen verschiedener Anfragen von Unternehmen und auch von mit der Abwicklung von Unternehmensinsolvenzen betrauten Insolvenzverwaltern wurde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit folgendes Problem herangetragen und um eine datenschutzrechtliche Lösung nachgesucht: Wie ist mit Kundendaten im Rahmen von Unternehmensverkäufen umzugehen?

Kundendaten haben einen erheblichen wirtschaftlichen Wert und stellen daher im Rahmen von Unternehmensverkäufen nicht selten

den hauptsächlichen Wert des Unternehmens dar. Auch im Hinblick auf die Veräußerung von Betriebsteilen oder werthaltigen Wirtschaftsgütern (sog. Assets) im Rahmen einer Insolvenz stellt sich diese Frage, weil auch hier der Wert in den vorhandenen Kundendatensätzen liegt.

In diesem Zusammenhang ist es jedoch notwendig, die datenschutzrechtlichen Grundsätze nicht außer Acht zu lassen, da Kundendaten keine „Ware“ sind, sondern dafür eigene gesetzliche Regelungen greifen.

Regelmäßig geht es dem Erwerber beim Unternehmenskauf darum, die Altkunden mittels Werbung ansprechen zu können. Die Datenübermittlung zu Werbezwecken ist in § 28 Abs. 3 Bundesdatenschutzgesetz (BDSG) abschließend geregelt. Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung ist zulässig, soweit der Betroffene eingewilligt hat. Sofern eine solche Einwilligung aber nicht vorliegt, ist darüber hinaus die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig zusammengefasste Daten handelt. Der Umfang der Kundendaten, die der Erwerber aufgrund dieser Vorschrift erhalten darf, ist daher auf die sog. Listendaten beschränkt. Bei den Listendaten handelt es sich um Name, Titel, akademischer Grad, Berufs-, Branchen- oder Geschäftsbezeichnung, Anschrift und Geburtsjahr, soweit sich diese Daten auf die Zugehörigkeit zu einer bestimmten Personengruppe beziehen. Auf dieser Grundlage dürfen aber nur die „Listendaten“ übergeben werden. Zusätzliche Daten wie Telefonnummern, E-Mail-Adressen oder Bankverbindungsdaten sind davon nicht umfasst.

In der Regel ist eine saubere, den Vorschriften des BDSG entsprechende Übermittlung von über die Listendaten hinausgehenden Kundendaten im Zuge eines Unternehmensverkaufs nur im Wege einer Einwilligung möglich, die den Voraussetzungen des § 4a BDSG entspricht. Die vom TLfDI vertretene Auffassung berücksichtigt dabei, dass bei dem alternativen Lösungsvorschlag, also einer Widerspruchslösung, nach hiesiger Auffassung nicht mit der notwendigen Wahrscheinlichkeit davon ausgegangen werden kann, dass schutzwürdige Belange der Betroffenen nicht überwiegen. Denn eine Widerspruchslösung bedeutet, dass der Betroffene dem Übergang seiner Daten widersprechen muss, um einen solchen zu verhindern und setzt daher ein Handeln des Betroffenen voraus. Handelt dieser jedoch nicht, sei es durch Änderung der Adressdaten, sei es durch

vorübergehende Abwesenheit, wird sein Schweigen „zu seinen Lasten“ gewertet, was bei einem so hohen Schutzgut wie dem informationellen Selbstbestimmungsrecht aus Art. 2 Abs. 1 Grundgesetz (GG) i. V. m. Art. 1 Abs. 1 GG als nicht vertretbar erscheint. Denn das Schweigen ist keine Erklärung und ein Dulden ist auch keine Handlung.

Ein besonderes Problem bei der Übernahme von Unternehmen stellen Arztpraxen und Rechtsanwaltskanzleien dar, da hier zum einen besondere Arten von personenbezogenen Daten in Form von Gesundheitsdaten im Raum stehen und zum anderen auf die Besonderheiten von Berufsgeheimnisträgern Rücksicht zu nehmen ist, dass in solchen Fällen eine Strafbarkeit nach § 203 Strafgesetzbuch (StGB) im Raum steht.

Der BGH hat für die Übergabe einer Patientenakte im Rahmen des Verkaufs einer Arztpraxis entschieden, dass die Weitergabe personenbezogener Daten in ärztlichen Behandlungsunterlagen, die grundsätzlich über intime Einzelheiten Aufschluss geben, zur Anwendung von § 203 Nr. 1 StGB führt (vgl. BGH in BGHZ 116, 268). Grundlage der Entscheidung BGHZ 116, 268 war die Bedeutung des Rechts des Einzelnen auf informationelle Selbstbestimmung und die daraus herzuleitende besondere Schutzbedürftigkeit personenbezogener Daten. Dies folgt sowohl – in Bezug auf Angehörige der Heilberufe sowie Rechtsanwälte – aus § 203 Nr. 1 StGB sowie ansonsten aus § 28 Abs. 2 BDSG. Unter Heranziehung dieser Wertungen des BGH in dem vergleichbar gelagerten Fall überwiegt das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Nutzung – hier also der Ausschluss der Weitergabe ohne Einwilligung – das Interesse des Datenverwenders. Bereits eine Rechtfertigung der Weitergabe der Daten mit dem objektiven Eigeninteresse der betroffenen Patienten an einer guten Fortführung ihrer Behandlung durch den neuen Arzt vermag nicht eine freie Entscheidung des Patienten zur Datenweitergabe zu ersetzen.

Beim Praxisverkauf oder bei der Praxisübernahme ist daher zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten hat. Der Verkauf einer Praxis oder die Insolvenz stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten muss es eine Einwilligungserklärung gem. § 4a BDSG aller Patienten geben. In der Praxis wird hier auf die sog. Zwei-Schränke-Methode zurückgegriffen. In einem Schrank werden

die Patientenakten des bisherigen Praxisinhabers aufbewahrt. Wenn der Patient nach der Praxisübernahme wieder zur Behandlung erscheint, wird er darüber aufgeklärt und er wird gefragt, ob er die Behandlung beim Praxiserwerber weiterführen möchte und dieser dazu in seine Patientenakte Einsicht nehmen darf. Wenn der Patient eine solche Einwilligung erteilt, dann wird die Akte im anderen Schrank, in dem des Erwerbers, abgelegt. Alle so gewanderten Akten stehen dann dem Erwerber als Patientenakten für seinen Praxisbetrieb zur Verfügung. Alle im ersten Schrank verbliebenen Akten bleiben dort und sind von dem Arzt, der die Praxis aufgibt, bis zum Ablauf der Aufbewahrungsfrist unter Verschluss zu halten.

Im Rahmen von Unternehmensveräußerungen oder Teilveräußerungen ist neben den wirtschaftlichen Aspekten auch stets auf die datenschutzkonforme Umsetzung dieser Veräußerungen zu achten. Auch im Hinblick auf eine wirtschaftliche und zeitnahe Lösung für die Unternehmen kann es im Hinblick auf die datenschutzrechtlichen Vorgaben nur eine Lösung geben: Die Übertragung von Kundendaten beim Unternehmenskauf ist grundsätzlich nur mittels einer Einwilligung gem. § 4a BDSG datenschutzkonform zu bewerkstelligen.

3.27 Datenschutz für Pseudonym?

Aufgrund der Beschwerde einer Mieterin erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis über einen möglichen Datenschutzverstoß seitens der in dem Mehrfamilienhaus tätigen Hausverwaltung. Die Beschwerdeführerin teilte dem TLfDI mit, dass die Hausverwaltung statt des von ihr aus diversen Gründen verwendeten Pseudonyms ihren richtigen Namen auf der für alle Mieter zugänglichen Haus- und Putzordnung vermerkt sowie die Nebenkostenabrechnung ebenfalls unter ihrem richtigen Namen versendet hatte. Darüber hinaus gab es in dem Mietshaus einen außen liegenden Gemeinschaftsbriefkasten, zu dem jeder Mieter einen Schlüssel hatte. Die Post wurde seitens der Mieter in die im Hausflur befindlichen Briefkästen umverteilt. Dabei kamen diverse Briefe und Post bei der Beschwerdeführerin gar nicht oder geöffnet an. Der TLfDI ermittelte durch ein Auskunftersuchen an die Hausverwaltung den Sachverhalt abschließend. Die Beschwerdeführerin teilte daraufhin mit, dass die Hausverwaltung zwischenzeitlich ihr Pseudonym nunmehr akzeptiert

habe und in der erforderlichen Weise verwenden würde. Die Beschwerde dahingehend hatte sich damit erledigt. Grundsätzlich gibt es keinen datenschutzrechtlichen Anspruch darauf, dass ein Vertragspartner statt des bürgerlichen Namens das von der betroffenen Person in der Öffentlichkeit benutzte Pseudonym verwendet. Eine solche Vereinbarung ist zivilrechtlich zwischen den Vertragspartnern zu vereinbaren, was im vorliegenden Fall nicht geschehen ist. Auch hinsichtlich der Problematik des Briefkastens und der geöffneten Briefe konnte kein datenschutzrechtlicher, sondern lediglich ein strafrechtlicher Verstoß gegen § 202 Strafgesetzbuch festgestellt werden, sodass dasungsverfahren gegen die Hausverwaltung beim TLfDI insgesamt abgeschlossen werden konnte.

Pseudonyme sind ebenfalls personenbezogene Daten i. S. d. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG). Hierüber ist eine Identifikation der betreffenden Person möglich. Diese sind daher auch vom Schutz des BDSG umfasst, welches nach § 1 Abs. 1 BDSG den einzelnen davor schützt, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Es gibt jedoch keinen datenschutzrechtlichen Anspruch des Betroffenen auf Verwendung dieses Pseudonyms. Hierfür ist eine zivilrechtliche Vereinbarung der einzelnen Vertragspartner erforderlich. Sofern bei der Verwendung dieses Pseudonyms Verstöße festgestellt werden, kann eine datenschutzrechtliche Überprüfung erfolgen.

3.28 Bürgerinitiative ratlos – der TLfDI kann helfen

Im Berichtszeitraum wandte sich eine Bürgerinitiative (BI) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie bat um datenschutzrechtliche Unterstützung bezüglich einer Unterschriftensammlung für die Errichtung eines Bestattungswaldes. Das Vorhaben konnte nicht realisiert werden, da die zuständige Thüringen Forst – Anstalt öffentlichen Rechts (AöR) das dafür notwendige Areal nicht zur Verfügung gestellt hatte. Die Unterschriftensammlung sollte an das Aufsichtführende Ministerium übergeben werden. Ziel dieses Bürgervotums sei es, das Anliegen der Bürgerinitiative (BI) für die Errichtung eines solchen Friedhofes mit überregionaler Bedeutung zu stützen. Die BI sah sich in Bezug auf die Erhebung und Nutzung von personenbezogenen

Daten im Rahmen der Unterschriftensammlung als verantwortliche Stelle im Sinne des § 2 Abs. 4 Bundesdatenschutzgesetz (BDSG). Da dieses Vorhaben für die BI von großer Bedeutung war und es nicht gefährdet werden sollte, wurde der TLfDI um datenschutzrechtliche Überprüfung gebeten.

Der TLfDI erklärte, dass sie als BI und damit Zusammenschluss mehrerer Personen mit einem gemeinsamen Zweck als Gesellschaft bürgerlichen Rechts einzuordnen ist. Als (teil-)rechtsfähige Personengesellschaft unterfällt diese damit auch den Regelungen des BDSG, soweit sie mit personenbezogenen Daten umgehe.

Der TLfDI gab zwei Möglichkeiten für eine datenschutzkonforme Unterschriftensammlung und die anschließende Übermittlung an das zuständige Ministerium vor:

Zum einen gibt es den sogenannten Erlaubnistatbestand. Demnach ist die angestrebte Unterschriftenliste von § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfasst. Danach ist die Datenerhebung und -übermittlung zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung überwiegen.

Das Sammeln der Unterschriften ist für diese BI erforderlich. Ein Überwiegen der Interessen der Unterschreibenden an einem Ausschluss der Verarbeitung, insbesondere der Übermittlung an das zuständige Ministerium, ist nicht ersichtlich, wenn auf diese beabsichtigte Folge hingewiesen wird, § 4 Abs. 3 BDSG. Einen solchen Hinweis enthielt das Schreiben der BI. Nicht gedeckt von § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Bekanntgeben (Übermitteln) von personenbezogenen Daten (andere Unterschriften) an einzelne, folgende Unterschreiber. Dies betrifft insbesondere die Information, wer noch auf der Liste unterschrieben hat. Daher ist die Liste auf geeignete Art und Weise abzudecken um eine (unbefugte) Übermittlung dieser Daten zu vermeiden. Der BI wurde geraten in ihrem Hinweis zu ergänzen, dass die Datenweitergabe ausschließlich an das zuständige Ministerium erfolgt.

Als zweite Möglichkeit wurde die Einwilligung erklärt. Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten verboten, es sei denn, eine Norm im BDSG oder eine andere Rechtsvorschrift erlaubt dies, ordnet dies an oder der/die Betroffene willigt in den Umgang mit seinen personenbezogenen Daten ein. Dies gilt auch, wenn private Stellen, zum Beispiel

Vereine, Unterschriften sammeln. Nach § 4a BDSG muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sollte eine Einwilligung zusammen mit anderen Einwilligungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Wegen der speziellen, im Gesetz eindeutig geregelten Voraussetzungen einer wirksamen Einwilligung ist hier jedoch pro unterschreibender Person ein Blatt zu nutzen. Dies liegt darin begründet, dass die Einwilligungen nicht auf dem Umfrageblatt erfolgen können und so ausgeschlossen ist, dass der Unterschreibende Kenntnis von anderen Einwilligenden nehmen kann. Zunächst hat die Person dann die Einwilligung auf diesem Blatt zu unterschreiben. Die Einwilligung hat sich vom übrigen Text auf geeignete Weise abzugrenzen, wie etwa mittels eines umlaufenden Kastens. Die Unterschrift muss als diesem Textstück zugehörig geleistet werden.

Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten verboten, es sei denn, eine Norm im BDSG oder eine andere Rechtsvorschrift erlaubt dies, ordnet dies an oder der/die Betroffene willigt in den Umgang mit seinen personenbezogenen Daten ein. Dies gilt auch, wenn private Stellen, zum Beispiel Vereine, Unterschriften sammeln. Da die Unterschriften in einer Liste erfasst werden, sind die bisherigen Unterschriften abzudecken, wenn eine neue Person unterschreibt. Somit kann der Folgeunterschreiber keine Kenntnis der bisherigen Unterschreiber erlangen.

3.29 Aktenlager überall

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein Hinweis über eine unsichere Aktenlagerung in einer Halle. Daraufhin wandte der TLfDI sich an das dortige Ordnungsamt mit der Bitte um Kontrolle des Gebäudes im Wege der Amtshilfe.

Gemäß § 9 Bundesdatenschutzgesetz (BDSG) hat die öffentliche oder nicht-öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die

in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Zu den organisatorischen Maßnahmen zählt unter anderem, dass sichergestellt wird, dass nur die Zugriffsberechtigten Einsicht in die Akten haben.

Die während der Kontrolle aufgenommenen Fotos zeigten, dass sich mehrere Gitterboxen voll mit Akten in der Halle befanden. Das Gebäude selbst war nicht begehbar; alle Türen und Tore waren verschlossen sowie die Fensterscheiben intakt. Somit hatte kein Dritter Zugang zu den Altakten.

Zu ermitteln war nun, wem die Akten gehörten, wem die Halle gehörte und ob die Akten überhaupt noch aufbewahrt werden müssen (Aufbewahrungsfristen). Die Ermittlung der verantwortlichen Stelle, also des Besitzers der Akten gestaltete sich schwierig. Firmenübernahmen und Verkäufe der Halle verlangsamten den Prozess. Nach einem erneuten Verkauf der Halle wurde dem TLfDI mitgeteilt, dass die Akten vernichtet worden seien. Erneut wurde das Ordnungsamt um eine Kontrolle gebeten. Bei dieser stellte sich heraus, dass tatsächlich alle Akten ausgeräumt waren.

Bei Verlassen eines Firmengebäudes wegen Verkaufs, Geschäftsaufgabe, etc. dürfen keine Akten zurückgelassen werden. Die Akten müssen archiviert und bei Ablauf der Aufbewahrungsfrist datenschutzgerecht vernichtet werden. Hierbei sind die Anforderungen an die Sicherheitsstufen der Schredder im Hinblick auf die Schutzklasse der Akten nach der DIN 66399 zu beachten.

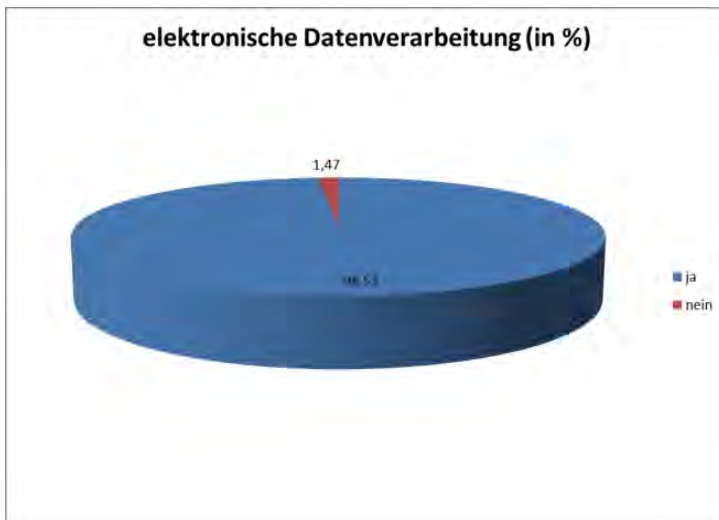
3.30 Umfrage des TLfDI – Thüringer Unternehmen zeigen sich hinsichtlich Datenschutzanforderungen höchst vorbildlich

Im Jahr 2016 führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Umfrage zum Thema „behördlicher Datenschutzbeauftragter“ i. V. m. „Datenübermittlung ins außereuropäische Ausland“ durch.

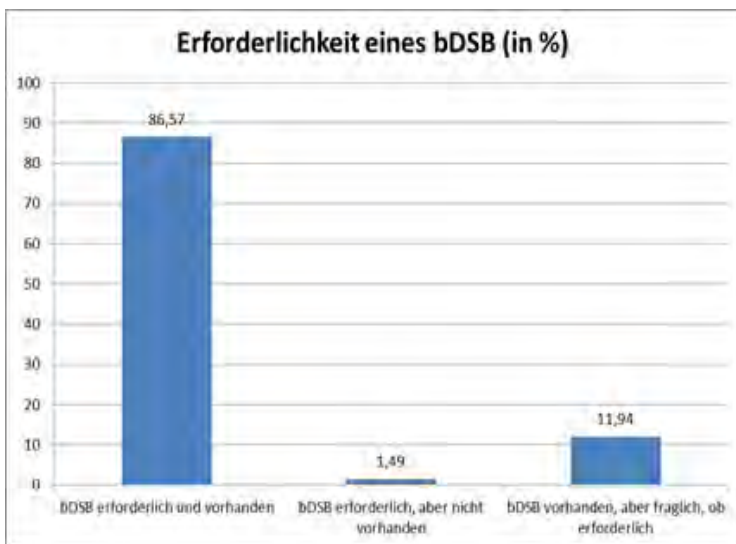
Hierbei wurden alle Thüringer Unternehmen mit mehr als 50 Beschäftigten angeschrieben. Mit der Umfrage hat sich der TLfDI einen Überblick über die Thüringer Datenschutzlandschaft in den abgefragten Bereichen verschafft.

Positiv hervorzuheben ist, dass 83 Prozent der Unternehmen sehr vorbildlich waren und ihrer Verpflichtung zur Antwort fristgemäß

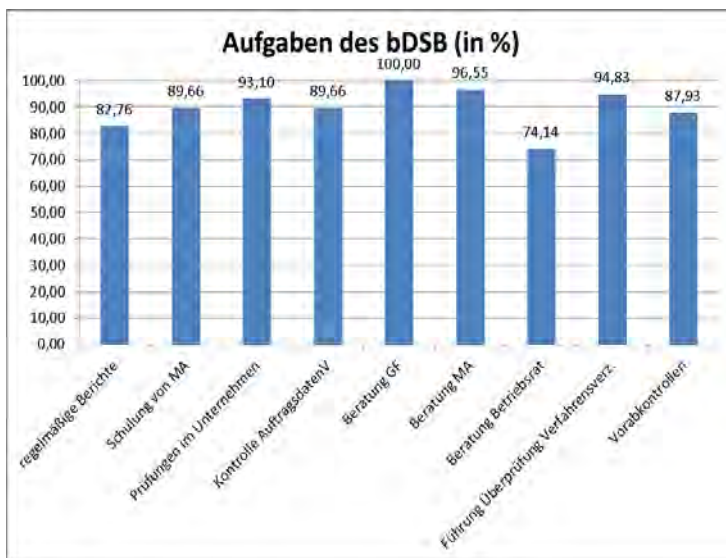
nachgekommen sind. Alle übrigen Unternehmen kamen der Aufforderung nach der ersten Erinnerung nach.



Der erste Teil des Fragebogens bezog sich auf die behördlichen Datenschutzbeauftragten (bDSB) und auf die Art und Weise, wie mit der Verarbeitung von personenbezogenen Daten umgegangen und verfahren wird. Nach dem Willen des Gesetzgebers haben bestimmte Unternehmen unter bestimmten Voraussetzungen einen solchen bDSB zu bestellen. Dieser muss wiederum bestimmten Kriterien entsprechen. Der TLfDI ist der Auffassung, dass der bDSB ein wichtiges Instrument für die Gewährleistung eines ausreichenden Datenschutzniveaus in Unternehmen ist, weswegen es auch besonders wichtig ist, dass die gesetzlichen Bestimmungen insoweit eingehalten werden. Die Umfrage hat ergeben, dass bei einer sehr deutlichen Mehrheit der Unternehmen ein bDSB erforderlich und vorhanden ist.



Positiv anzumerken ist hierbei, dass es bei 86 Prozent der Angeschriebenen nichts im Hinblick auf die Bestellpflicht eines bDSB zu bemängeln gibt. Auch in Bezug auf die Vereinbarkeit des bDSB mit dessen hauptberuflicher Tätigkeit im Unternehmen ist bei 97 Prozent der Unternehmen alles im grünen Bereich. Wer als bDSB bestellt ist und daneben noch andere Tätigkeiten im Unternehmen ausübt, darf nämlich keine Aufgaben wahrnehmen, die zu Interessenskonflikten bei der Tätigkeit als bDSB führen. Klassisches (Negativ-)Beispiel hierfür ist die Bestellung des IT-Leiters oder gar des Geschäftsführers als bDSB.



In der Grafik ist gut erkennbar, welche Aufgaben die behördlichen Datenschutzbeauftragten im Rahmen ihrer Tätigkeit erledigen.

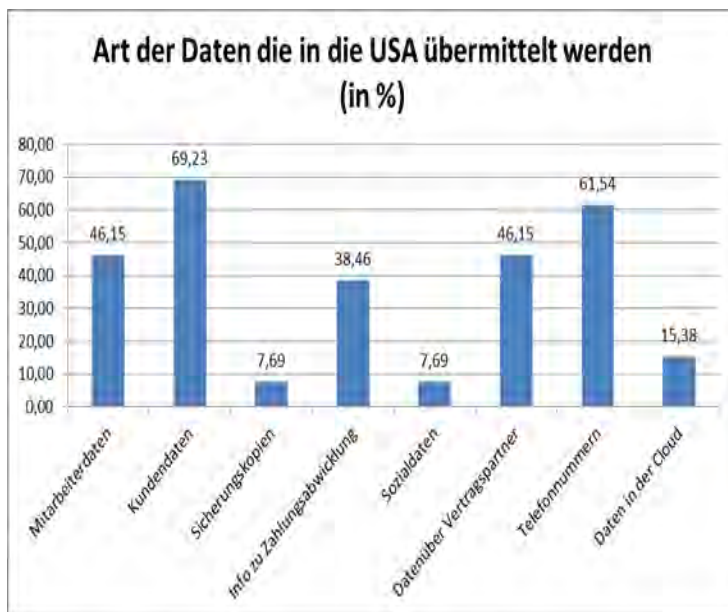
Auch im Hinblick auf die Weiterbildung der bDSB in den Unternehmen gibt es seitens des TLfDI fast nichts zu meckern. Denn 86 Prozent der bDSB gehen regelmäßig zu Fortbildungen. Dies ist gerade zu dem jetzigen Zeitpunkt, also dem Ausklingen des Bundesdatenschutzgesetzes (BDSG) bis zum Mai 2018 und ab dann dem Gelten der DS-GVO, unverzichtbar.

Bis auf wenige Einzelfälle hat die Umfrage also ein positives Bild auf Thüringens größere Unternehmen geworfen. Sie sind in Sachen bDSB gut aufgestellt und wissen in der Regel auch, was ihre Pflichten sind.

Der andere Bereich, den die Umfrage abprüfen sollte, war die Übermittlung von personenbezogenen Daten insbesondere in die USA. Hier ist nach Auswertung der Umfrage festzustellen, dass 2/3 der befragten Unternehmen nach eigenen Angaben überhaupt keine personenbezogenen Daten in die USA übermitteln. Etwa drei Prozent der Unternehmen machten hierzu keine Angaben, hier wird der TLfDI in Einzelfällen nochmals nachhaken. Das bedeutet

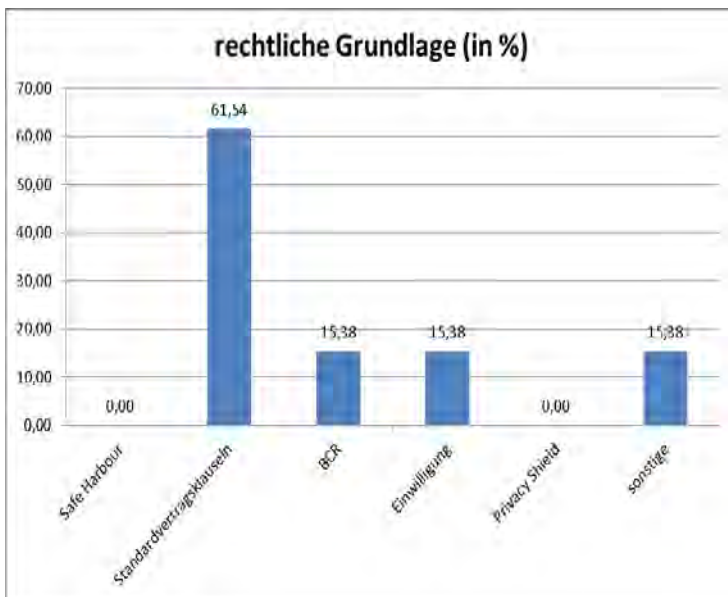
im Umkehrschluss, dass etwa 19 Prozent der Unternehmen diese sensiblen Daten in die USA übermitteln.

Übermittelt werden übrigens, wie sich der folgenden Grafik entnehmen lässt, vornehmlich Mitarbeiterdaten und Kundendaten.

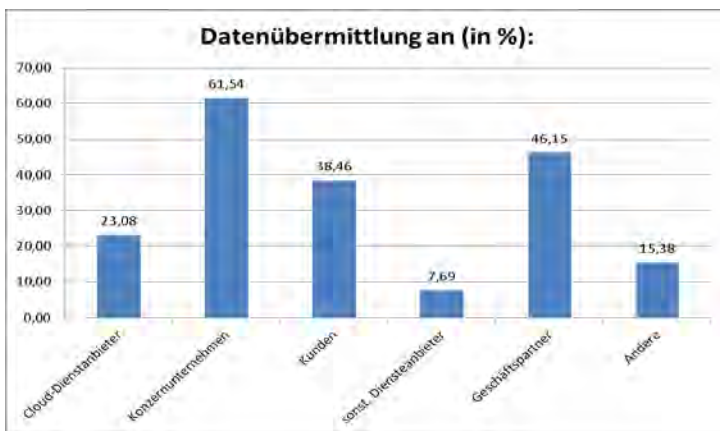


Anhand der Grafik lässt sich die Art der Daten gut erkennen. Nicht überraschend ist, dass Kundendaten, Daten über Vertragspartner und Mitarbeiterdaten weit vorne liegen.

Doch auf welcher rechtlichen Grundlage erfolgt dies? 61 Prozent rechtfertigen dies mit dem Hinweis auf Standardvertragsklauseln. Jeweils 15 Prozent berufen sich auf Einwilligungen, Binding Corporate Rules (BCR). Unter „Sonstige“ gaben die Unternehmen Vertragsklauseln und § 4c Abs. 1 BDSG an. Die Prüfungen hierzu hat der TLfDI noch nicht abgeschlossen.



Übermittelt werden die Daten übrigens an verschiedene Empfänger. In der folgenden Grafik ist das Ziel der Datenübermittlung gut erkennbar. Unter „Andere“ wurden US-Steuerbehörden, SWIFT und sonstige Diensteanbieter seitens der Unternehmen benannt.



Zusammenfassend für den Bereich „Datenübermittlung ins außereuropäische Ausland“ kann man sagen, dass es eher bei einem kleinen Kreis der Thüringer Unternehmen eine Rolle spielt. Es ist davon auszugehen, dass in kleineren Unternehmen noch weniger Daten in die USA übermittelt werden.

Inwieweit die Übermittlungen durch die einzelnen, befragten Unternehmen rechtmäßig sind, wird vom TLfDI geprüft werden.

Diese Umfrage war das erste Mal, dass der TLfDI sich dieses Instruments bedient hat, um sich einen breiten Überblick zu verschaffen, wie die Datenschutzlandschaft in Thüringen in bestimmten Bereichen ausgestaltet ist. Das Ergebnis war nach derzeitigem Kenntnisstand erfreulich. Den wenigen Einzelfällen, in denen die Antworten oder Stirnrunzeln bei den Prüfern hervorgerufen haben, wird in naher Zukunft nachgegangen werden. Es ist auch nicht auszuschließen, dass dieses Instrument erneut genutzt wird, um einzelne Sparten gezielt zu prüfen.

3.31 Weitergabe von Kundenverbrauchsdaten durch Versorgungsunternehmen

Im Berichtszeitraum wandte sich ein Versorgungsunternehmen an den Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es erhielt von einer thüringischen Stadtverwaltung die Anfrage, Verbrauchsdaten von Kunden herauszugeben wegen des Verdachts auf dauerhaft illegale Wohnungsnutzungen. Dies geschah außerhalb eines offiziellen Ermittlungsverfahrens. Das Versorgungsunternehmen lehnte die Bitte um Auskunft ab und erbat sich vom TLfDI eine Bestätigung der Rechtsauffassung bzw. um eine Stellungnahme, falls diese abweichen sollte.

Messdaten, die mit Zählern ermittelt werden, sind auch personenbezogene Daten i. S. d. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG). Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Ursprünglich wurden die Messdaten für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses

ses mit dem Betroffenen erhoben und verarbeitet (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Für die Übermittlung der personenbezogenen Daten an die Stadtverwaltung käme sodann als Erlaubnisnorm § 28 Abs. 2 Nr. 2 BDSG infrage. Demnach ist eine Übermittlung von personenbezogenen Daten für einen anderen Zweck nur zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten (Buchstabe a) oder zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist (Buchstabe b) und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Das Versorgungsunternehmen rechtfertigte die Ablehnung mit folgenden Gründen:

Das illegale Bauen oder Nutzen von baulichen Anlagen stellt nach der Thüringer Bauordnung eine Ordnungswidrigkeit und keine Straftat dar. Der Gesetzgeber hat ausdrücklich davon abgesehen, Ordnungswidrigkeiten in den Katalog der zulässigen Zweckänderungen mit aufzunehmen. Somit ist § 28 Abs. 2 Nr. 2 Buchstabe b BDSG nicht einschlägig.

Zweifelsfrei ist die Ermittlung von illegalem Wohnungsbau und illegaler Wohnungsnutzung ein berechtigtes Interesse der Stadtverwaltung (Buchstabe a). Allerdings besteht durchaus ein Grund zur Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung seiner Daten hat. Solch ein Interesse ist immer dann anzunehmen, wenn Daten übermittelt werden sollen, die sich auf strafbare Handlungen, Ordnungswidrigkeiten oder arbeitsrechtliche Verhältnisse beziehen.

Der TLfDI stimmt der Rechtsauffassung zu und führt ergänzend aus, dass eine Beurteilung, ob der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, immer am Einzelfall zu erfolgen hat. Die Angaben der Stadtverwaltung „um gegen illegale, dauerhafte Wohnnutzungen vorzugehen“ ist viel zu abstrakt, um eine Einzelfallprüfung vornehmen zu können. Ebenso wird von der Stadtverwaltung nicht konkret angegeben, welche Rechtsverstöße genau vorliegen.

Folglich wäre die Situation anders zu bewerten, wenn die Stadtverwaltung ein offizielles Verwaltungsverfahren einleitet und eindeutig darlegen kann, welche Rechtsverstöße gegeben sind und damit eine konkrete Gefahr für die öffentliche Sicherheit bestünde. Bei Gefahr für die öffentliche Sicherheit wird es nahezu unmöglich, die Verar-

beutung von Daten aufgrund von Interessen der Betroffenen abzulehnen.

Aber auch dann hat die Stadtverwaltung ihrerseits eine Ermächtigungsnorm zu nennen, die sie zur Erhebung der Daten berechtigt.

Die Datenerhebung und nachfolgende Verarbeitung hat immer zweckgebunden zu erfolgen (§ 28 Abs. 1 S. 2 BDSG). Eine zweckfremde Übermittlung oder Nutzung ohne Einverständnis des Betroffenen ist nur in engen Grenzen und nur soweit das Gesetz dies ausdrücklich regelt zulässig (siehe § 28 Abs. 2 BDSG).

3.32 Schrott sammeln = Daten sammeln? Fortsetzung II

Seit sechs Jahren beschäftigt sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Fall der Anfertigung von Personalausweiskopien bei einem Metall-Recycling-Unternehmen.

Im 2. Tätigkeitsbericht des TLfDI zum Datenschutz: Nicht-öffentlicher Bereich endete der Beitrag damit, dass das Unternehmen Rechtsmittel einlegte (s. a. 2. TB TLfDI: Nicht-öffentlicher Bereich [2.27]).

Die fortwährende Diskussion drehte sich erneut um die Frage, in welchem Umfang das Schrottunternehmen Daten erheben darf. Nachdem das Erstellen von Personalausweiskopien nach Anordnung eingestellt wurde, ging das Unternehmen dazu über, ein Formblatt von den Lieferanten ausfüllen zu lassen. Hierin wurden folgende Daten abgefragt: Name, Vorname, Straße, PLZ/Ort, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Personalausweisnummer, Gültigkeit des Personalausweises.

Gemäß § 4 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Das Unternehmen trug vor, dass es, um seiner Benennungspflicht nach § 160 Abgabenordnung (AO) nachzukommen, notwendig sei, diese Daten zu erheben. Gemäß § 160 AO sind Schulden und andere Lasten, Betriebsausgaben, Werbungskosten und andere Ausgaben steuerlich regelmäßig nicht zu berücksichtigen, wenn der Steuerpflichtige dem Verlangen der Finanzbehörde nicht nachkommt, die Gläubiger oder die Empfänger genau zu benennen. Allerdings zählt

§ 143 AO abschließend auf, welche Daten von Unternehmen bei Wareneingängen aufgezeichnet werden müssen. Gefordert sind lediglich der Name oder die Firma und die Anschrift des Lieferers (§ 143 Abs. 3 Nr. 2 AO) sowie weitere Daten zur Lieferung an sich. Daraufhin erwiderte das Unternehmen, dass während Betriebsprüfungen mehrfach von Finanzbehörden Kopien von Personalausweisen gefordert wurden. Jedoch besagt die ständige Rechtsprechung der Finanzgerichte und des Bundesfinanzgerichtshofs eindeutig, dass nach § 160 AO der Name und die Anschrift vollkommen ausreichend sind. Die Unternehmen sollen nicht aus Angst vor steuerrechtlichen Nachteilen durch Betriebsausgabenabzug vorbeugende Ermittlungsaufgaben für das Finanzamt wahrnehmen.

Auf die steuerrechtlichen Normen lässt sich eine Erhebung und Speicherung von Daten über den Namen oder die Firma und die Anschrift des Lieferers folglich nicht stützen.

Da sich das Unternehmen nicht überzeugen ließ, ordnete der TLfDI an, dass nur noch die Daten erhoben werden sollen, die der Gesetzgeber in der Abgabenordnung vorschreibt. Gegen diesen Anordnungsbescheid erhob das Unternehmen Klage beim zuständigen Verwaltungsgericht.

In der mündlichen Verhandlung wurden die Punkte nochmals problematisiert. Das Verwaltungsgericht wies die Klage des Unternehmens ab und bestätigte die Rechtsauffassung des TLfDI.

Unternehmen sind in bestimmten Fällen verpflichtet, gewisse Daten über ihre Kunden zu erheben, um Betriebsausgaben steuerrechtlich geltend zu machen. Dabei hat der Gesetzgeber vorgegeben, welche Daten dies sind. Darüber hinaus dürfen Unternehmen keine Daten erheben, da es hierfür keine Erlaubnisnorm gibt.

3.33 Handy als Navigator im Einkaufszentrum – beim TLfDI läuten die Alarmglocken

Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) aus der Presse Kenntnis darüber, dass an einem Pilotprojekt gearbeitet wird. In einem Einkaufszentrum solle das Handy den Kunden durch das Zentrum führen. Das Smartphone solle zudem – jeweils vor dem entsprechenden Schaufenster – auf besondere Aktionen hinweisen. In diesem Presseartikel wurde erklärt, dass man um die neuen Tech-

nologien wüsste und man im Handel nicht auf der Stelle treten dürfe, wenn man vorne mit dabei sein wolle. Man wolle die richtige Information zum richtigen Zeitpunkt „an den Mann“ bringen. Mit entsprechenden Minisendern im gesamten Einkaufszentrum soll es möglich werden, den Standort der Kunden zu „ermitteln“ und somit eine mögliche Navigation zu ermöglichen. Die Kunden könnten durch eine entsprechende App selbst entscheiden, ob sie diesen Service nutzen möchten und sich somit durch das Center leiten lassen. Aber damit nicht genug. Weiterhin soll auch das Umfeld mit eingebunden werden. Von der Parkplatzsuche bis zum Nahverkehr.

Beim Datenschutz klingelten daraufhin alle Alarmglocken. Also wandte man sich an das Management des Centers. Man wollte im Vorfeld die datenschutzrechtlichen Auswirkungen des geplanten Systems mit dem Management besprechen. Im Zuge dessen wurden alle technischen Details – sofern schon bekannt – zum künftigen System erfragt.

Das Management erklärte daraufhin, dass derzeit eine App entwickelt wird, die die Kunden über Neuigkeiten und Ereignisse im Einkaufszentrum informieren soll. Zudem bietet die App eine Reihe von ortsbasierten Diensten an. Hierzu zählen die Positionsbestimmung des Kunden im Einkaufszentrum und die Navigation zu einem gewünschten Ziel. Damit wird dem Kunden des Centers eine bessere Orientierung ermöglicht. Um die Funktion der App zu optimieren, muss der Nutzer sein Geschlecht und sein Alter angeben. Bezüglich der Einwilligung zur Nutzung der Daten gemäß § 4a Bundesdatenschutzgesetz muss jeder Nutzer beim Installieren der App die Datenschutzbestimmungen akzeptieren.

Der TLfDI wandte sich erneut an das Management des Centers, um noch mehr Details zur technischen Ausstattung der App in Erfahrung zu bringen.

Der Fall befindet sich derzeit noch in Bearbeitung. Ob diese App und die damit verbundene Verwendung im Sinne des Datenschutzes sind, bleibt abzuwarten. Der TLfDI bleibt jedenfalls dran.

Die Zuständigkeit des TLfDI beschränkt sich nicht nur auf bereits stattfindende Datenverarbeitung. Vielmehr kann er bereits im Vorfeld beratend tätig sein oder bei sich abzeichnenden schweren Verstößen gegen das Datenschutzrecht auch schon dann tätig werden, wenn es noch nicht zu einer Rechtsverletzung gekommen ist.

3.34 Öffentlich zugänglich aufgestellte Container mit Akten eines Steuerbüros in Gera

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von einer Thüringer Landespolizeiinspektion (LPI) mitgeteilt, dass zwei Datentonnen mit der Beschriftung „Datenträger zu vernichten“ frei zugänglich im öffentlichen Raum stehen würden. Dies wurde der Polizei durch einen aufmerksamen Bürger mitgeteilt. Die eingeleiteten Ermittlungen der Polizei bestätigten diesen Zustand. Bei einem Container war es ohne Umstände möglich, an entsprechende Akten zu gelangen. Die Polizeibeamten stellten fest, dass zumindest einer der beiden Behälter möglicherweise bauliche Mängel aufweist, welche eine Entnahme von Dokumenten aus dem Behälter ermöglichen würde. Die Container konnten einem Steuerbüro zugeordnet werden. Die Verantwortlichen wurden hinzugezogen und das sichere Verwahren der Akten wurde überwacht.

Der Bürger teilte wenige Stunden später der Polizei erneut mit, dass nun Teile des Inhaltes der besagten Tonnen für jedermann zugänglich im öffentlichen Raum aufgefunden worden sein sollen. Wie und wann diese Unterlagen aus den Behältern in die Öffentlichkeit gelangen konnten, konnte durch die Beamten vor Ort nicht festgestellt werden. Die an die Polizeibeamten übergebenen Dokumente wurden sichergestellt. Die Polizei bat den TLfDI um datenschutzrechtliche Prüfung.

Der TLfDI wandte sich daraufhin an das Unternehmen und forderte die Übersendung der Unterlagen zu allen technischen und organisatorischen Maßnahmen, die zur Gewährleistung der Regelungen des Bundesdatenschutzes (BDSG) in diesem Unternehmen getroffen wurden. Insbesondere wollte der TLfDI wissen, wie der Umgang mit zu vernichtenden Unterlagen geregelt wurde.

Das Unternehmen teilte dem TLfDI mit, dass die sensiblen Daten von einem beauftragten Unternehmen vernichtet werden sollten. Es wurden dafür vorgesehene Container bestellt. Die Behälter wurden mit Dokumenten gefüllt, ordnungsgemäß verschlossen und zur vereinbarten Abholung bereitgestellt. Das Entsorgungsunternehmen hatte die Container jedoch nicht wie vereinbart abgeholt. Über die Presse erfuhr dann das Unternehmen, dass aus den verschlossenen Containern Dokumente entwendet wurden.

Das Unternehmen konnte keinen Verstoß gegen die Anforderungen des Datenschutzes nach Bundesdatenschutzgesetz erkennen. Vielmehr träfe die Verantwortung wohl das Unternehmen, das mit der Vernichtung der Unterlagen beauftragt war und diese nicht abgeholt hatte.

Der TLfDI teilte dem Unternehmen mit, dass es selbst verantwortliche Stelle nach § 3 Abs. 7 BDSG bleibt, auch wenn es personenbezogene Daten durch andere im Auftrag verarbeiten lässt. Dies gilt auch für den Fall von Datenvernichtung. Von einer solchen verantwortlichen nicht-öffentlichen Stelle sind technische und organisatorische Maßnahmen vorzunehmen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten. Hierzu zählt ausdrücklich die Gewährleistung nach Ziffer 3 zweiter Halbsatz der Anlage zu § 9 Satz 1 BDSG, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Durch die Lagerung von personenbezogenen Daten in den Datensicherheitsbehältern im öffentlichen Raum kam es zur Kenntnisnahme dieser personenbezogenen Daten durch Dritte und letztendlich zur Beschlagnahme durch die Polizeibehörde. Im Ergebnis waren die getroffenen technisch organisatorischen Maßnahmen daher nicht ausreichend.

Ein Steuerberater unterliegt nach § 203 Absatz 1 Strafgesetzbuch (StGB) einem besonderen Berufsgeheimnis. Das bedeutet, wer unbefugt das Privatgeheimnis verletzt, wie beispielsweise durch die Offenbarung eines fremden Geheimnisses, eines namentlich zum persönlichen Lebensbereich gehörenden Geheimnisses oder eines Betriebsgeheimnisses seiner Mandanten, kann mit einer Freiheitsstrafe bis zu einem Jahr oder einer Geldstrafe bestraft werden. Eine solche Verletzung würde dann vorliegen, sobald ein Dritter – in diesem Fall der mit der Vernichtung der Akten beauftragte Mitarbeiter des Vernichtungsunternehmens – Kenntnis vom Inhalt der Akten erlangen würde. Dies wäre zweifelsfrei beim Herausnehmen der Akten aus den Behältern der Fall.

Die Vernichtung oder sonstige Verarbeitung von personenbezogenen Daten, die einem besonderen Berufsgeheimnis unterfallen, kann rechtlich einwandfrei nur dann durch Beauftragung eines Drittunternehmens realisiert werden, wenn eine Kenntnisnahme des Akteninhalts durch das Drittunternehmen zu 100 Prozent ausgeschlossen ist. Dies liegt darin begründet, dass mit der Übergabe der Daten an ein

Drittunternehmen regelmäßig der objektive Straftatbestand des § 203 StGB erfüllt ist. Damit ist der in solchen Fällen zur Auftragsdatenverarbeitung zu schließende und zwingend vorausgesetzte Vertrag über die Auftragsdatenverarbeitung gemäß § 11 BDSG nach § 134 Bürgerliches Gesetzbuch wegen eines bestehenden gesetzlichen Verbotes nichtig. Ohne einen solchen Vertrag über die Auftragsdatenverarbeitung ist eine Vernichtung der betreffenden Daten aber rechtlich nicht in zulässiger Art und Weise realisierbar.

Nach Kenntnis des TLfDI ist derzeit ein Gesetzgebungsverfahren im Gange, dass auf eine Änderung des § 203 StGB abzielt. Damit sollen auch Berufsgeheimnisträger in die Lage versetzt werden, Dritte als Auftragsdatenverarbeiter einzusetzen.

Das Steuerbüro teilte dem TLfDI daraufhin mit, dass es nunmehr alle zu vernichtenden Unterlagen vor Ort mittels eines Büroschredders vernichten würde. Dieser entspricht der Sicherheitsstufe 4 nach DIN 32757-1. Das geschredderte Material weist demnach eine Materialteilchenfläche kleiner/gleich 30 Quadratmillimeter auf.

Da damit sichergestellt wurde, dass eine Kenntnisnahme durch Dritte ausgeschlossen ist, war eine weitere Tätigkeit des TLfDI nicht erforderlich.

Ein Steuerberater unterliegt nach § 203 Absatz 1 Strafgesetzbuch einem besonderen Berufsgeheimnis. Die Vernichtung oder sonstige Verarbeitung von personenbezogenen Daten ist besonders zu beachten. Der Steuerberater ist bis zur letztlichen Unkenntlichmachung seiner zur Vernichtung abgegebenen Akten verantwortlich. Er hat dafür Sorge zu tragen, dass niemand Kenntnis vom Inhalt der Akten erhält. Dies ist beim Abgeben der Akten in den Datencontainern schwer zu kontrollieren. Der entsprechende Mitarbeiter des Aktenvernichtungsunternehmens könnte Kenntnis vom Inhalt der Akten erlangen. Dies kann verhindert werden, indem die Akten vor Entsorgung geschreddert werden.

3.35 Onlineshops: Kreditkartendaten frei Haus?

Der Bayerische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (BayLfDI) informierte seine Länderkollegen, darunter auch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), über eine Medienmeldung, wonach zahlreiche Onlineshops (Internethandel) mit Kredit-

karten-Skimmern „verseucht“ sind. Sicherheitslücken bei Online-shop-Betreibern würden ausgenutzt, um Skimming-Wanzen zu implementieren und damit Kreditkartendaten abzugreifen. Dem BayLfDI lag eine Liste vor, wieviele und welche Onlineshops in den Bundesländern von den Angriffen betroffen waren.

Der TLfDI bat den BayLfDI um Information, ob und welche Onlineshops in Thüringen betroffen sind. Die vom BayLfDI übersandten Informationen ergaben, dass in Thüringen lediglich ein Onlineshop von den Hackerangriffen und der Ausspähung von Kreditkartendaten betroffen war.

Nach § 42 Abs. 1 i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI datenschutzrechtlich die zuständige Aufsichtsbehörde i. S. d. § 38 Abs. 1 BDSG für Unternehmen. Im Rahmen seiner Aufsicht überwacht der TLfDI die Einhaltung des BDSG und anderer datenschutzrechtlicher Vorschriften bei nicht-öffentlichen Stellen in Thüringen und somit auch Privatunternehmen. Daher wandte sich der TLfDI schriftlich an den Betreiber des betroffenen Thüringer Onlineshops und informierte ihn darüber, dass in einem Artikel des Online-Magazins heise.de (<https://www.heise.de/newsticker/meldung/Ueber-1000-deutsche-Online-Shops-infiziert-und-angezapft-3592281.html>) vom 10. Januar 2017 von

potenziellen Sicherheitslücken bei Online-Shops berichtet wird, die von Cyber-Kriminellen ausgenutzt werden könnten. Diesbezüglich verwies der TLfDI auf die veröffentlichte Liste der betroffenen Shops (<https://gitlab.com/gwillem/public-snippets/snippets/28813/raw>), die auch die betriebenen Domains des



Thüringer Internethandels enthielt.

Der TLfDI wies den Unternehmer darauf hin, dass auf seinen betriebenen Domains eine Shop-Software in einer nicht-ausreichend gesicherten Version eingesetzt wird und die vorhandenen Sicherheitslücken von Cyberkriminellen bereits ausgenutzt werden. Eine Prüfung durch den TLfDI hatte ergeben, dass

auch sein Internethandel mit Schadsoftware infiziert war, die Kreditkartendaten an Kriminelle übermittelt. Details, welches Skript diese Übermittlung ausführt, waren jedoch nicht bekannt.



Der TLfDI empfahl dem Betreiber des Onlineshops, sofort die Shop-Software im aktuellen Status zu sichern, um Beweise gegenüber Dritten zwecks Schadensersatz zu bewahren. Der TLfDI wies den Unternehmer auf eine Internetseite hin, die eine detaillierte Anleitung zur Lösung des Problems enthielt,



<https://support.hypernode.com/knowledgebase/how-to-fix-credit-card-hijack/> und auf die Seite <https://www.magereport.com>.

Auf dieser Seite konnte der Unternehmer den aktuellen Sicherheitsstatus seines Shops nachprüfen.

Abschließend forderte der TLfDI den Onlineshop-Betreiber auf, den Schadcode zu entziffern und zu entfernen, sofern dies nicht möglich sein sollte, müsste die Shop-Software neu installiert werden. Im Hinblick darauf bat der TLfDI den Shop-Betreiber um eine Mitteilung, welche Maßnahmen er getroffen hatte und um die Übersendung einer gepackten Sicherheitskopie der Shop-Software (nur die PHP-Skripte, HTML-Code und Javaskripte – ohne Datenbanken und Zugangsdaten).

Der Betreiber des Internethandels teilte dem TLfDI daraufhin schriftlich mit, dass in seinem Onlineshop keine Kreditkartendaten erhoben werden und erhoben wurden; als einzige Zahlungsart biete er Vorkasse mit Überweisung an. Somit hatte der Betreiber nach eigener Darlegung nie Zahlungsdaten von Kunden erhoben oder gespeichert, die hätten ausgespäht werden können. Dem



Kunden wurden lediglich die Bankdaten des Betreibers mitgeteilt. Somit fand die Zahlung an seine Bank durch den Kunden außerhalb des Shop-Systems statt.

Weiterhin informierte der Unternehmer den TLfDI darüber, dass er sich aufgrund der Hacker-Angriffe dennoch entschieden hatte, zukünftig ein alternatives Shop-System zu verwenden und dies bereits angelegt hatte.

Mit der Umstellung auf ein anderes Shop-System erklärte der TLfDI gegenüber dem Onlineshop-Betreiber die datenschutzrechtliche Erledigung des Vorgangs.

Nach § 42 Abs. 1 i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI datenschutzrechtlich die zuständige Aufsichtsbehörde i. S. d. § 38 Abs. 1 BDSG für nicht-öffentliche Stellen und somit auch Privatunternehmen. Der TLfDI kann gegenüber Privatunternehmen technische Maßnahmen anordnen, um die Einhaltung datenschutzrechtlicher Bestimmungen zu gewährleisten.

3.36 Datenschutz auch beim Schornsteinfeger

Im Berichtszeitraum erreichte den Thüringer Beauftragten für den Datenschutz und die Informationsfreiheit die Beschwerde eines Schornsteinfegermeisters. Er meldete, dass der Geselle des ehemaligen für den Kehrbezirk zuständigen Schornsteinfegers, der sich mittlerweile zur Ruhe gesetzt hatte, ein Rundschreiben zur Kundengewinnung an ehemalige Kunden verschickte. Diesem Anschreiben war ein Flyer beigelegt, der die Serviceleistungen des Unternehmens des Gesellen beschreibt sowie eine vorbereitete personalisierte Vertragsausfertigung für die Kunden zur sofortigen Unterschrift und zur Beauftragung mit den Schornsteinfegerarbeiten an deren Liegenschaften.

Der Beschwerdeführer äußerte den Verdacht, dass der Geselle die Daten aus dem Bestand des Schornsteinfegers, für den er tätig gewesen ist, übernommen hätte.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Der TLfDI wandte sich mit einem Auskunftersuchen an den Gesellen und bat um Stellungnahme. Dieser antwortete, dass er durch seine jahrelange Tätigkeit, als Geselle im Betrieb des Schornsteinfegermeisters Kenntnis von den Daten erlangt hatte. Zudem hatte er handschriftliche Karteikarteien geführt, auf denen die Kundendaten notiert wurden: die Anschrift, die Termine, die Art der Feuerstätten und die erledigten Aufgaben. Mithilfe dieser Karteikarten, war es ihm möglich, die Anschreiben an die Kunden zu fertigen und die Werbung für sein Unternehmen zu versenden. Von den Kunden wurden vorab allerdings keine schriftlichen Einwilligungserklärungen zur werblichen Nutzung ihrer Daten eingeholt.

Der TLfDI prüft derzeit, inwieweit eine Rechtsgrundlage zur Nutzung der Daten bestanden haben könnte. Über den Ausgang der Prüfung wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

3.37 Datenübermittlung von Makler zu Makler – Der TLfDI bezieht Stellung!

Im Berichtszeitraum erreichte ein Schreiben eines Versicherungsunternehmens einige Datenschutzbeauftragte des Bundes und der Länder. Das Versicherungsunternehmen bat um Information darüber, wie eine Bestandsübertragung eines Versicherungsmaklers bei z. B. Tod, Insolvenz, Geschäftsaufgabe oder Verkauf an einen anderen Versicherungsmakler im Einklang mit dem Bundesdatenschutzgesetz (BDSG) erfolgen kann.

Der TLfDI vertritt hierzu folgende Auffassung:

Beim Übergang eines Maklergeschäfts von der gekauften Gesellschaft auf die übernehmende Gesellschaft und bei der damit verbundenen Übertragung der Kundendaten ist zunächst die Art der Daten, die übertragen werden sollen, von Bedeutung und ob diese Daten ggf. als ganzer Datensatz oder auch als Teile von Kundendatensätzen übertragen werden können.

Für die Übertragung der Datensätze ist § 28 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) i. V. m. § 28 Abs. 1 S. 1 Nr. 2 BDSG für das abgebende Unternehmen und § 28 Abs. 1 S. 1 Nr. 2 BDSG für das übernehmende Unternehmen als einschlägige Rechtsgrundlage anzusehen, soweit keine Gesundheitsdaten betroffen sind.

In die Interessenabwägung zwischen dem berechtigten Interesse der verantwortlichen Stelle, also dem Versicherungsunternehmen, und dem schutzwürdigen Interesse der Betroffenen ist allerdings nach Auffassung des TLfDI folgendes mit einzubeziehen: Die Betroffenen dürfen keinem Kontrahierungszwang ausgesetzt werden. Die Übertragung eines Versicherungsmaklers liegt im Ermessen des Betroffenen. Auch steht es ihm gewöhnlich frei, sich diesen auszusuchen. Der Betroffene ist nicht gehalten, mit einem bestimmten Makler eine vertragliche Beziehung einzugehen. Der Betroffene kann auch jeder-

zeit ohne Makler mit dem Versicherungsunternehmen seiner Wahl einen Versicherungsvertrag abschließen. Der Weg über den Makler mag zwar für den Kunden bequemer sein, ist aber nicht notwendig. Es liegt daher nicht ohne weiteres auch im Interesse des Betroffenen, dass er die Daten, die er einem Makler anvertraut hat, einem anderen, für ihn unbekannten Makler zur Verfügung stellen will. Das schutzwürdige Interesse des Betroffenen geht zweifelsfrei dahin, dass seine wirtschaftlichen, sozialen und beruflichen Daten nicht unnötig offen gelegt werden. Insoweit wird es als notwendig angesehen, dieser Interessenlage im Besonderen gerecht zu werden. Daher müssen die schutzwürdigen Interessen der Betroffenen durch die Einräumung eines Widerspruchsrechts und einer angemessenen Widerspruchsfrist, die auch längere Urlaube berücksichtigt, gewahrt werden.

Das Widerspruchsrecht muss allerdings auch bestimmten Anforderungen genügen. Es ist ähnlich wie bei der Einwilligung notwendig, dass dem Betroffenen mitgeteilt wird, an wen, wann und zu welchem Zweck welche Daten übertragen werden sollen. Es ist ihm gleichwohl mitzuteilen, dass sein Vertrag auch ohne die Inanspruchnahme eines neuen Maklers weiterbesteht, da nur so dem Eindruck von Zwang entgegengesteuert werden kann. Erst nach dem Fristablauf können dann ggf. die Übertragungen der Daten, gestützt auf § 28 Abs. 2 Nr. 1 BDSG, vorgenommen werden.

Als Problem bei dieser Art der Wegbereitung für die Anwendung von § 28 Abs. 2 Nr. 1 BDSG für die Übermittlung von Kundendaten wird allerdings im Bereich der Versicherungen gesehen, dass es eine Vielzahl von Betroffenen gibt, die sich lediglich für den Vertragsabschluss eines Maklers bedient haben, diesen aber sonst nie wieder bemüht haben. Insoweit ist fraglich, ob ein Schreiben mit der Aufforderung zum Widerspruch z. B. mangels aktueller Zustelladresse die schutzwürdigen Interessen des Betroffenen in ausreichendem Maße wahren kann, da hier die Einräumung des Widerspruchsrechts wohl ins Leere geht.

Für den Bereich der Übermittlung von Gesundheitsdaten ist auf jeden Fall eine explizite Einwilligung der Betroffenen erforderlich. Diese Einwilligung ist an die Voraussetzungen des § 4a BDSG geknüpft. Hierin heißt es, dass eine Einwilligung nur dann wirksam ist, wenn diese auf einer freien Entscheidung des Betroffenen beruht. Diese Einwilligung bedarf der Schriftform. Der Betroffene ist auf eventuelle Folgen bei einer nicht erfolgten Einwilligung hinzuwei-

sen. Sollte es sich gemäß § 4a Absatz 3 BDSG i. V. m. § 3 Absatz 9 BDSG um eine besondere Art der personenbezogenen Daten handeln, wie beispielsweise Gesundheitsdaten, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Oftmals werden Kundendaten bei Unternehmensverkäufen freigiebig mitverkauft oder stillschweigend im Unternehmen belassen. Dieses Vorgehen ist datenschutzrechtlich oftmals mit schwerwiegenden datenschutzrechtlichen Verstößen verbunden, die auch vom TLfDI in Thüringen verfolgt und geahndet werden. Es lohnt daher vorher ein Blick ins Gesetz, um die notwendigen Voraussetzungen für die Weitergabe der Daten zu schaffen. Oder ein Anruf beim TLfDI ☺

3.38 Digitale Unterschriften versus Datenschutz

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Presseanfrage eines Onlineportals. Der TLfDI wurde gebeten, eine Stellungnahme zur Rechtmäßigkeit von digitalen Unterschriften in Versicherungsverträgen abzugeben. Anbei wurde ein Fragenkatalog zur Beantwortung geschickt. Es stellte sich heraus, dass mehrere Landesaufsichtsbehörden diese Anfrage erhielten. Daraufhin einigte man sich auf eine gemeinsame, abgestimmte Positionierung im Rahmen der ständigen Arbeitsgruppe für Versicherungswirtschaft.

Grundsätzlich ist die Wirksamkeit von Verträgen eine zivilrechtliche Fragestellung. Erst bei Verträgen, die auch die Verarbeitung von personenbezogenen Daten regeln, gilt es die Normen des Bundesdatenschutzgesetzes (BDSG) zu beachten. Eine Einwilligung zur Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten muss gem. § 4a BDSG in Schriftform erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die hier genannte Schriftform entspricht den Vorgaben des § 126 Bürgerliches Gesetzbuch.

Eine digitale Unterschrift, die auf einem Unterschriften-Pad mittels Touch-Eingabe gezeichnet wird, ist keine schriftliche Erklärung in dem Sinne. Es fehlt dem Touch-Display an der Fähigkeit, Schriftzeichen dauerhaft festzuhalten. Zu beachten ist auch, dass ein besonderer Umstand i. S. d. § 4a Abs. 1 BDSG nicht schon vorliegt, weil es bequemer ist, eine Unterschrift digital zu verwalten oder beide Parteien im Einvernehmen auf die zivilrechtliche Schriftform verzich-

ten. Ebenso stellt die Unterschrift auf dem Unterschriften-Pad keine qualifizierte elektronische Signatur im Sinne des Signaturgesetzes dar. Die qualifizierte elektronische Signatur ist ein algorithmisches Verfahren, das einen Buchstaben- und Zahlencode mit dem zu signierenden Dokument verbindet. Nur dieses Verfahren kann eine eigenhändige Unterschrift ersetzen.

Außerdem müssen Versicherer den Vorschriften des Versicherungsvertragsgesetzes nachkommen. Auch hier wird an zahlreichen Stellen eine schriftliche Erklärung verlangt.

Jedenfalls ist datenschutzrechtlich immer darauf zu achten, dass bei jeder Datenverarbeitung ein legitimer Zweck verfolgt wird. Für diesen Zweck muss eine Rechtsgrundlage oder die Einwilligung des Betroffenen vorliegen. Auch müssen die personenbezogenen Daten der Versicherten in technischer sowie organisatorischer Hinsicht vor dem Zugriff durch Unbefugte (z. B. andere Sachbearbeiter der Organisation) geschützt werden. Hierbei sind die Vorgaben des § 9 BDSG, welcher die Festlegung von technischen und organisatorischen Maßnahmen regelt, einschließlich der Anlage 1 zu § 9 BDSG zu beachten.

Die Gültigkeit eines Vertrages und die Bindungswirkung der verschiedenen Formvorgaben ist eine zivilrechtliche Fragestellung. Erst wenn Verträge auch die Verarbeitung von personenbezogenen Daten regeln, sind die datenschutzrechtlichen Vorgaben zu beachten (§§ 4, 4a BDSG). Für die Erhebung, die weitere Verarbeitung und Nutzung der personenbezogenen Daten hat die verantwortliche Stelle die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Daten vor dem Zugriff von Dritten zu schützen (siehe § 9 BDSG samt Anlage).

3.39 Schreddern? – Aber richtig?

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Thüringer Vereins hinsichtlich der gesetzlichen Vorgaben für die Aufbewahrung und Vernichtung von Akten mit personenbezogenen Daten und besonderen Arten von personenbezogenen Daten, z. B. Daten zur ethnischen Herkunft, zu politischen Meinungen, zu religiösen Überzeugungen, zur Gewerkschaftszugehörigkeit und zu Gesundheitsdaten. Zunächst unterliegt auch die Vernichtung der Akten dem Bun-

desdatenschutzgesetz (BDSG), da die Vernichtung eine Form der Datenverarbeitung ist, nämlich eine Datenlöschung, § 3 Abs. 4 Nr. 5 BDSG.

Dem Verein wurde auf seine Anfrage hin mitgeteilt, dass die Aufbewahrung von derart sensiblen Daten in Aktenform oder in Form von elektronisch gesicherten Daten auf einem Speichermedium grundsätzlich in einem verschließbaren Behälter stattfinden muss. Hierzu ist grundsätzlich auch ein Tresor geeignet. Zu diesem dürfen dann aber auch nur solche Personen Zugang haben, die die Berechtigung zum Umgang mit den Akten haben. Andere Personen sind vom Zugriff auszuschließen.

In Sachen Aktenvernichtung wurde dem Verein mitgeteilt, dass es im Rahmen der Vernichtung von Datenträgern wichtig ist, dass die DIN 66399-1 „Büro- und Datentechnik – Vernichtung von Datenträgern“ Berücksichtigung findet. Sie beschreibt die Anforderungen an Maschinen und Einrichtungen zur Vernichtung von Informationsträgern. Je nach dem Grad der Schutzbedürftigkeit der auf dem Datenträger oder in der Akte gespeicherten Informationen werden fünf Sicherheitsstufen definiert. Die Stufe P-3 ist dabei nur als eine Mindestanforderung für die datenschutzgerechte Vernichtung anzusehen. Für sensible personenbezogene Daten ist aber aus Sicht des TLfDI (und weiterer zehn deutscher Datenschutzbehörden) mindestens die Sicherheitsstufe P-5 erforderlich. Der Schredder, der dieser Sicherheitsstufe entspricht, zerteilt das Material in eine Teilchengröße kleiner/gleich 30 qmm. Bei dieser Sicherheitsstufe ist von einer datenschutzkonformen Vernichtung durch die verantwortliche Stelle auszugehen.

Soll die Vernichtung nicht durch die verantwortliche Stelle selbst, sondern durch einen externen Dienstleister erfolgen, muss im Rahmen der Beauftragung zur Vernichtung der Akten an den Abschluss eines Auftragsdatenverarbeitungs-Vertrages (ADV-Vertrages) gemäß § 11 Abs. 2 BDSG gedacht werden, da dieser zwingend notwendig ist. Die Vernichtung der Akten stellt eine Verarbeitung im Auftrag durch andere dar. Dieser Vertrag ist schriftlich abzufassen und muss die notwendigen Angaben enthalten, welche sich aus § 11 Abs. 2 Nr. 1-10 BDSG ergeben.

Zu beachten ist allerdings, dass gem. § 1 Abs. 3 S. 2 BDSG die Verpflichtung zur Wahrung gesetzlich vorgesehener Geheimhaltungspflichten oder von besonderen Berufs- und Amtsgeheimnissen bestehen bleibt. Diese Pflichten, die insbesondere in § 203 Strafgesetz-

buch ausdrückliche Erwähnung finden, bestehen neben den Vorschriften des BDSG. Die Auslagerung der Datenvernichtung an einen externen Dienstleister mittels eines ADV-Vertrages, kann daher eine unzulässige Offenbarung von Geheimnissen darstellen, selbst wenn die Voraussetzungen für eine Auftragsverarbeitung vorliegen.

Auch für die Vernichtung von Akten gelten die Vorschriften des BDSG, da die Vernichtung eine Form der Verarbeitung, nämlich der Löschung darstellt. Es gelten daher auch für die Vernichtung von Akten die Pflichten der verantwortlichen Stelle. Die verantwortliche Stelle hat daher die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, die für die Umsetzung des BDSG erforderlich sind. Bei Aktenvernichtungen, die besondere Arten personenbezogener Daten beinhalten, ist darauf zu achten, dass diese auch nach dem Schreddern nur eine Materialteilchengröße von kleiner/gleich 30 qmm aufweisen und damit den Anforderungen an die Sicherheitsstufe P-5 der DIN 66399-1 genügen.

3.40 Hilferuf eines Vereins aus dem datenschutzrechtlichen Dickicht

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine breit gefächerte Anfrage eines Thüringer Vereins hinsichtlich verschiedener datenschutzrechtlicher Problemstellungen, angefangen bei den besonderen Anforderungen an eine Einwilligung zur Datennutzung, die Formulierung einer Datenschutzerklärung, der Versendung von Newslettern an seine Vereinsmitglieder sowie die zulässige Nutzung von Fotos für die Website des Vereins.

Die datenschutzrechtliche Einwilligungserklärung und die Hinweise zum Datenschutz sind dabei sachlich verschiedene Dinge, die nicht miteinander vermischt werden dürfen. Es ist daher zwischen einem reinen Datenschutzhinweis und zwischen einer datenschutzrechtlichen Einwilligungserklärung zu trennen. Ein entsprechendes Formblatt, welches an die Mitglieder ausgegeben werden soll, muss dies auch redaktionell berücksichtigen. Der Betroffene muss in dem Formblatt zur Einwilligung klar und verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle

informiert werden. Ebenfalls ist auf die Folgen einer eventuellen Verweigerung der Einwilligung hinzuweisen (§ 4a Abs. 1 Satz 2 Bundesdatenschutzgesetz [BDSG]). Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent in der Einwilligungserklärung zu erläutern. Weiterhin ist zu beachten, dass eine wirksame Einwilligung gem. § 4a BDSG auch nur dann vorliegt, wenn diese freiwillig abgegeben wurde und jederzeit widerrufen werden kann. Auf diese Möglichkeit ist ebenfalls explizit hinzuweisen. Schlussendlich sollte auch die Erklärung selbst eindeutig und aus sich heraus verständlich sein. Es ist eine Formulierung zu wählen, die dem Betroffenen bewusst macht, dass er eine zusätzliche Erklärung abgibt. Es sollte auch möglichst eine Einwilligungserklärung erstellt werden, die alle Zwecke der möglichen Verwendung beinhaltet. Für jeden einzelnen Zweck, also für werbliche Ansprache, Newsletter, für Veröffentlichung von Daten im Internet, für das Lastschriftverfahren usw., wird eine gesonderte Erklärung abgefragt und jeweils auf die Widerruflichkeit hingewiesen. Jede einzelne Erklärung kann dann entweder vom Betroffenen unterschrieben und damit die Einwilligung erteilt werden, oder eben nicht. Eine Vielzahl von einzelnen Einwilligungserklärungen trägt nicht zur Transparenz bei und birgt die Gefahr, dass die Einholung einzelner Erklärungen auch vergessen werden kann. Bei der Datenschutzerklärung hingegen handelt es sich um die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz bzw. Vertrag.

Der Verein wollte seine Mitglieder zukünftig auch gerne in einem Newsletter über alles rund um den Verein informieren. Dieser Newsletter sollte aber gleichermaßen an die bestehenden und die neuen Mitglieder versandt werden. Die Voraussetzungen dafür sind jedoch unterschiedlich. Zunächst ist bei den bestehenden Mitgliedschaften von einer rechtmäßigen Erhebung der Adressdaten der E-Mail-Adresse ausdrücklich für Vereinszwecke, d. h. für die Übersendung von Informationen über alle Belange des Vereins, auszugehen. Diese Informationsübermittlung kann dann auch mithilfe des Newsletters geschehen. Beachtet werden muss jedoch, dass dieser Newsletter dann keine „Werbung“ darstellt und ausschließlich vereinsinterne Mitteilungen enthält, die vom Vereinszweck gedeckt sind und damit durch die Versendung eigene Geschäftszwecke des Vereins gemäß § 28 Abs. 1 Nr. 1 BDSG erfüllt werden.

Enthält der Newsletter Werbung, so ist eine Nutzung der E-Mail-Adresse nur unter den Voraussetzungen des § 28 Abs. 3 ff. BDSG möglich. Da es sich bei der E-Mail-Adresse nicht um listenmäßig zusammengefasste Daten über Angehörige einer bestimmten Personengruppe, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken (privilegiertes Listendatum) handelt, wird daher dann zwingend die Einwilligung der jeweiligen Person, § 28 Abs. 3 Satz 1 BDSG, benötigt. Auch muss in den Fällen der Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG und bei jeder Ansprache des einzelnen Mitglieds zum Zwecke der Werbung über das Widerspruchsrecht belehrt werden, § 28 Abs. 4 Satz 2 BDSG. Diese Belehrung ist dann an die „Bestandsmitglieder“ bereits vor der ersten werblichen Ansprache zu erteilen, da bereits hierfür und dann ohne vorherige Belehrung die E-Mail zum Zwecke der Werbung genutzt werden würde. Bei den neuen Mitgliedern würde man diese Einwilligung zur werblichen Ansprache natürlich vorab, schon bei Beantragung der Mitgliedschaft, einholen. Dem Verein wurde daher angeraten, dass Einwilligungsformular entsprechend anzupassen.

Eine weitere Frage betraf die Verwendung von Fotos, welche im Rahmen von Veranstaltungen wie Messen oder anderen öffentlichen Anlässen gemacht werden. Diese Fotos sollen dem Verein für seine Vereinschronik zur Verfügung stehen. Hierbei wurden von den Personen, die jeweils fotografiert worden sind, mündliche Zustimmungen eingeholt. Fraglich war seitens des Vereins, ob dies ausreichend ist und was passiert, wenn ein Betroffener auf einem Foto nicht zustimmt. Da der Verein im Zweifel die rechtmäßige Verwendung der Fotos nachzuweisen hat, ist es auf jeden Fall notwendig, dass die Einwilligung zur Nutzung und/oder Veröffentlichung der Fotos schriftlich niedergelegt wird. Daraus lässt sich auch zweifelsfrei der jeweilige Umfang der Nutzungsberechtigung ersehen. Ein grundsätzliches Löschen des gesamten Fotos, wenn eine Einwilligung nicht gegeben wurde, ist nicht notwendig. Es genügt dann, wenn der Einzelne stark verpixelt dargestellt oder anderweitig unkenntlich gemacht wird (Balken).

Der Verein hat zusammen mit dem TLfDI seine Formulare und Erklärungsblätter überarbeitet und seinen Mitgliedern daraufhin überarbeitet zur Verfügung gestellt.

Die datenschutzrechtliche Einwilligungserklärung und die Hinweise zum Datenschutz sind sachlich verschiedene Dinge, die nicht miteinander vermischt werden dürfen. In der Einwilligungserklärung muss klar und verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informiert werden. Ebenfalls ist auf die Folgen einer eventuellen Verweigerung der Einwilligung hinzuweisen. Für jeden einzelnen Zweck, also für werbliche Ansprache, Newsletter, für Veröffentlichung von Daten im Internet, für das Lastschriftverfahren usw., wird eine gesonderte Erklärung abgefragt und jeweils auf die Widerruflichkeit hingewiesen.

3.41 Vereinsberatung

Im Berichtszeitraum wandte sich ein beratender Verein an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er erbat eine Beratung zu seinem Umgang mit Datenflüssen sowie die Klärung von Fragen zu datenschutzrechtlichen Bestimmungen, um seine Arbeit zu optimieren.

Gemäß § 38 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse.

Um den Umgang mit personenbezogenen Daten datenschutzrechtlich bewerten zu können, mussten zunächst die genauen Datenflüsse und Beratungssachverhalte geklärt werden. Hierfür traf sich der TLfDI mit Vertretern der Beratungsstelle. Zu klärende Fragen waren unter anderem: Auf welche Ermächtigungsnormen stützen sich die Erhebung, Verarbeitung und Übermittlung von personenbezogenen Daten und besonderer Arten von personenbezogenen Daten (siehe § 3 Abs. 9 BDSG).

Werden schriftliche Einwilligungserklärungen der Betroffenen eingeholt?

Außerdem wurde die Beratungsstelle gebeten darzulegen, wie und welche Daten erhoben werden, warum diese erforderlich sind, wie diese Daten dann weiterverarbeitet werden und, falls eine Übermittlung der Daten stattfindet, an wen diese Übermittlung erfolgt. Zudem sollte erklärt werden, welche technischen und organisatorischen Maßnahmen getroffen wurden, um das Bundesdatenschutzgesetz umzusetzen (gem. § 9 BDSG i. V. m. der Anlage). Des Weiteren

sollte die Beratungsstelle ausführen, welchen Aufbewahrungsfristen die erhobenen Daten unterliegen und auf welche Art und Weise die Löschung vorgenommen wird. Die Beratungsstelle kam dem nach und reichte hierfür verschiedene Unterlagen ein. Diese Unterlagen werden nun vom TLfDI auf ihre Vereinbarkeit mit dem BDSG hin geprüft. Nach der Feststellung eines möglichen Änderungsbedarfs wird der TLfDI eine abschließende datenschutzrechtliche Beurteilung treffen. Über den Ausgang wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Nach § 38 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Verantwortliche Stellen, also Unternehmen und Personen, die personenbezogene Daten erheben, verarbeiten und übermitteln, können sich bei Unsicherheiten im Umgang mit Daten mit ihren Fragen immer an den TLfDI wenden.

3.42 Herrenlose Akten eines Bauunternehmers

Der behördliche Datenschutzbeauftragte (bDSB) eines Thüringer Landratsamtes (LRA) wandte sich im Namen des Bauordnungsamtes des LRA an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Bei der Begehung einer Abbruchimmobilie hatte das Bauordnungsamt zwei Schränke mit diversen Aktenordnern gefunden. Aufgrund des sehr maroden Gebäudezustands und der Gefahr für die öffentliche Sicherheit und Ordnung beabsichtigte das Bauordnungsamt einen kurzfristigen Rückbau. Als Eigentümer der Immobilie war im Grundbuch eine GmbH eingetragen, deren Prokurist verstorben war und deren Geschäftsführer sich im Ausland befand. Das Bauordnungsamt hatte jedoch keine Zustelladresse herausfinden können.

Im Hinblick auf den Datenschutz und den unbekannten Inhalt der Aktenordner im Gebäude bat der bDSB den TLfDI um Auskunft darüber, ob der Landkreis die Akten sicherstellen müsse (beispielsweise im Archiv) und wer Akteneinsicht erhalten dürfe. Zur Erläuterung übersandte der bDSB dem TLfDI Fotos der Aktenschränke im Gebäude.

Der TLfDI führte im Rahmen der Amtshilfe zunächst eine gemeinsame Begehung der Immobile mit dem Bauordnungsamt des LRA

durch. Dabei wurden ca. 50 Aktenordner festgestellt, die einem Bauunternehmen und dessen Komplementärin (persönlich haftender Gesellschafter einer Kommanditgesellschaft) zugeordnet werden konnte. Der TLfDI bat die zuständigen Gewerbeämter um nähere Auskunft zum Status der Unternehmen. Das Gewerbeamt informierte den TLfDI darüber, dass beide angefragten Firmen abgemeldet seien und teilte dem TLfDI die genauen Adressen der früheren Firmensitze mit. Die zu diesem Zeitpunkt bestehende Adresse der Geschäftsführerin war auch bekannt. Beide Gesellschaften waren bereits aus dem Handelsregister gelöscht worden, wodurch auch die eingetragenen Liquidatoren seit diesem Zeitpunkt nicht mehr bestellt waren.

Aufgrund dieser Informationen wandte sich der TLfDI an das Einwohnermeldeamt und bat um Mitteilung, ob die Adresse der letzten Geschäftsführerin noch aktuell ist. Das Einwohnermeldeamt teilte dem TLfDI die aktuelle Adresse der letzten eingetragenen Geschäftsführerin mit.

Aufgrund der ihm nunmehr vorliegenden Informationen teilte der TLfDI dem Bauordnungsamt des Landkreises mit, dass die Geschäftsführerin wegen ihrer nicht vollständig durchgeführten Liquidation und der im Abbruchgebäude verbliebenen Akten u. U. als Störerin im ordnungsrechtlichen Sinne in Betracht komme. Dies müsse durch die hierfür zuständige Behörde geprüft werden. Sofern Tatbestände von Ordnungswidrigkeiten vorliegen, können diese auch verjährt sein.

Nach Auffassung des TLfDI tragen Liquidatoren einer GmbH auch eine Verantwortung im Sinne des Datenschutzrechts, da sie verpflichtet sind, die Geschäfte der Gesellschaft abzuwickeln und somit zumindest die verantwortliche Stelle entsprechend einem Geschäftsführer vertreten. Allerdings kann eine solche Verantwortlichkeit im Sinne des Bundesdatenschutzgesetzes (BDSG) nicht mehr greifen, wenn die zu liquidierende Gesellschaft gelöscht und damit die Liquidatoreneigenschaft ebenfalls erloschen ist.

Zur Abwicklung der Angelegenheit und zu einer möglichen Aufforderung, die Akten aus dem Gebäude zu entfernen, teilte der TLfDI dem Bauordnungsamt des Landkreises die aktuelle Meldeadresse der letzten Geschäftsführerin im Rahmen der Amtshilfe mit. Der TLfDI kündigte an, die frühere Geschäftsführerin über die Abgabe ihrer Meldeadresse gemäß § 21 Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) zu informieren und bat das Bauordnungsamt, ihn über

den Ausgang des Verfahrens in Kenntnis zu setzen. Eine derartige Information hat den TLfDI noch nicht erreicht.

Nach Auffassung des TLfDI tragen Liquidatoren einer GmbH auch eine Verantwortung im Sinne des Datenschutzrechts, da sie verpflichtet sind, die Geschäfte der Gesellschaft abzuwickeln und somit zumindest die verantwortliche Stelle entsprechend einem Geschäftsführer zu vertreten. Allerdings kann eine solche Verantwortlichkeit im Sinne des Bundesdatenschutzgesetzes (BDSG) nicht mehr greifen, wenn die zu liquidierende Gesellschaft gelöscht und damit die Liquidatoreneigenschaft ebenfalls erloschen ist. Sofern nach der Löschung festgestellt wird, dass die Vernichtung bzw. Abwicklung von Unternehmensakten datenschutzrechtlich nicht ordnungsgemäß erfolgte, sind Tatbestände einer Ordnungswidrigkeit zu prüfen.

3.43 Nachhilfe: Bürger erhält Auskunft

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Hilfe. Er hatte sich mit der Bitte um Auskunft nach § 34 Bundesdatenschutzgesetz (BDSG) über die zu seiner Person gespeicherten Daten an eine Firma gewandt. Nach § 34 Abs. 1 BDSG hat jedermann einen Auskunftsanspruch gegen verantwortliche Stellen. Dieser Anspruch beinhaltet die zu einer Person gespeicherten Daten, die Herkunft der Daten, den Empfänger, an den diese Daten weitergegeben werden und den Zweck der Speicherung.

Die Firma beantwortete die vom Beschwerdeführer gestellten Fragen allerdings nicht, weswegen dieser sich hilfesuchend an den TLfDI wandte. Der TLfDI kontaktierte daraufhin mit einem Auskunftsverlangen nach § 38 BDSG das Unternehmen und bat um Auskunft darüber, welche Daten zu dessen Person gespeichert, woher diese Daten bezogen, an wen diese Daten weitergegeben und zu welchem Zweck diese Daten gespeichert wurden. Gleichzeitig wurde das Unternehmen vom TLfDI über den Inhalt der Auskunftspflicht nach § 34 BDSG belehrt.

Das Unternehmen reagierte auf das Auskunftsverlangen rasch und erklärte dem TLfDI die Vorgehensweise bei Anfragen nach § 34 BDSG. Es hätte bereits einigen Kunden solche Auskünfte erteilt, weswegen ihnen das Prozedere nicht unbekannt sei. In der Regel würden solche Anfragen innerhalb einer Woche beantwortet. Des

Weiteren versicherte das Unternehmen, dass es durchaus wüsste, dass es diese Auskünfte zu erteilen habe und auch keinen Grund sähe, dies nicht zu tun. Allerdings teilte das Unternehmen mit, dass es diese Anfrage des Bürgers nicht erhalten habe. Es konnte die Anfrage auch nicht anhand des Namens finden. Der TLfDI übersandte deshalb – mit Zustimmung des Bürgers – das Auskunftersuchen erneut an das Unternehmen, woraufhin der Bürger seine erwünschten Auskünfte erhielt.

Am Ende bedankte sich der Bürger beim TLfDI für die unkomplizierte und schnelle Hilfe. Damit war das Verfahren abgeschlossen. Die Aussage, man habe das Schreiben des Bürgers nicht erhalten, ließ sich nicht widerlegen, da es per E-Mail versandt wurde. Aus diesem Grund wurden gegenüber dem Unternehmen auch keine weiteren Maßnahmen ergriffen.

Gemäß § 34 Abs. 1 BDSG sind die verantwortlichen Stellen dem Betroffenen gegenüber verpflichtet, auf dessen Verlangen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, sowie über den Empfänger, an den die Daten weiter gegeben werden und über den Zweck der Speicherung Auskunft zu erteilen. Die Auskunft umfasst auch die Mitteilung, dass, sollte dies der Fall sein, über den Betroffenen keine Daten gespeichert sind (sog. Negativauskunft). Der TLfDI rät dazu, solche Auskunftersuchen immer in einer Art und Weise zu versenden, die den Zugang dokumentiert. Am besten per Einschreiben mit Rückschein. Dabei sollte dem Unternehmen eine angemessene Frist zur Bearbeitung eingeräumt werden. In der Regel ist hierbei ein Zeitraum von zwei Wochen anzusetzen.

3.44 Keine Lastschrift ohne Daten

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde einer Kundin über das Lastschriftverfahren in einem Einzelhandelsgeschäft.

Zur Klärung des Sachverhalts führte der TLfDI eine unangekündigte Vor-Ort-Kontrolle nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) durch. Während des Gesprächs mit dem Geschäftsführer erklärte sich dieser nach anfänglichen Vorbehalten auch mit der Kontrolle einverstanden. Daraufhin erklärte er den Ablauf eines

Lastschriftverfahrens in seinem Ladengeschäft. Der Kunde wird beim Zahlvorgang mittels Lastschrift nach Name und Anschrift gefragt. Diese Angaben werden vom Verkäufer in die elektronische Kasse (Computerkasse) eingegeben, um dann einen Beleg drucken zu können. Auf dem Lastschriftbeleg werden dann neben der Kontonummer, der Bankleitzahl und dem Betrag auch der Name und die Adresse des Einkaufenden erfasst.

Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine schriftliche Einwilligung, wie vom Gesetzgeber gefordert, wird vorliegend nicht eingeholt. Als einzige Erlaubnisnorm für die hier vorgenommene Datenerhebung und Speicherung käme § 28 Abs. 1 Satz 1 Nr. 1 BDSG infrage. Gemäß dieser Vorschrift ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Allerdings sind Name und Anschrift nicht erforderlich, um das Schuldverhältnis zwischen dem Kunden und dem Einzelhandelsgeschäft zu begründen, durchzuführen oder zu beenden. Auch für den eventuellen Fall der Nichteinlösung einer Lastschrift sind diese zusätzlichen Daten nicht erforderlich. Für die Abwicklung eines Lastschriftverfahrens sind die mittgeteilten Kontodaten ausreichend. Im Falle der Nichteinlösung der Lastschrift wird die Bank des Kunden durch dessen Unterschrift bevollmächtigt, an den Verkäufer die zur Verfolgung des Anspruchs notwendigen personenbezogenen Daten herauszugeben. Das zusätzliche Erfassen von Adresse und Name des Kunden auf dem Lastschriftbeleg ist daher zur Verfolgung des Anspruchs auf Zahlung nicht erforderlich, da der Verkäufer ohne Weiteres von der Bank diese Daten auf Nachfrage erhält. Insoweit stellt daher das Vermerken der zusätzlichen Daten auf dem Beleg einen datenschutzrechtlich unzulässigen Vorgang dar.

Gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendi-

gung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Ein Unternehmen ist daher nur dazu berechtigt, die zur Durchführung einer Kaufhandlung notwendigen Daten zu erheben und zu nutzen.

3.45 Jeder kennt jeden – Hausverwaltung gibt Daten weiter

Im Berichtszeitraum beschwerte sich ein Bürger über seine Hausverwaltung. Er erhielt ein Mieterhöhungsschreiben seiner Hausverwaltung. Hierbei wurden zur Ermittlung der ortsüblichen Miete, drei sogenannte Vergleichsobjekte im selben Gemeindegebiet benannt. Diese Vergleichsobjekte enthielten in ihrer Beschreibung den vollständigen Namen der derzeitigen Mieter, die vollständige Adresse mit Angabe der Etage, die Wohnfläche und den Mietzins pro Quadratmeter. Der Bürger kritisierte zudem, dass man durch die Daten – wie Größe der Wohnung und den monatlichen Mietzins – durchaus Rückschlüsse auf die Einkommensverhältnisse ziehen könnte.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wandte sich mit einem Auskunftsverlangen an die Hausverwaltung. Der TLfDI wollte in Erfahrung bringen, aufgrund welcher Rechtsgrundlage die vollständigen Namen der Mieter der Vergleichsobjekte benannt wurden und bei welchen weiteren Mieterhöhungsschreiben die personenbezogenen Daten des Bürgers wiederum als Referenzobjekt für eine Mieterhöhung angegeben wurden.

Die Hausverwaltung erklärte, dass die rechtliche Grundlage in § 558a Absatz 2 Nummer 4 des Bürgerlichen Gesetzbuchs (BGB) zu finden sei. Danach könne zur Begründung der Mieterhöhung Bezug auf entsprechende Entgelte für einzelne vergleichbare Wohnungen genommen werden, dabei genüge die Nennung von drei Wohnungen. Weiterhin gab die Hausverwaltung an, dass eine Voraussetzung für die Erhöhung nach der Vergleichsmiete sei, dass der Mieter die genannten Wohnungen eindeutig identifizieren kann. Der Mieter müsse nachvollziehen können, dass die geforderte Vergleichsmiete korrekt ist. Insbesondere bei Mehrfamilienhäusern ist es notwendig, auch den Namen des Mieters anzugeben. Hierzu führt der Bundesgerichtshof in seiner Entscheidung vom 20. September 1982 (BGHZ 84, 392) sowie vom 28. März 2012 (BGH WuM 2003, 149) aus, dass der Vermieter hierzu mindestens folgende Angaben machen muss: Anschrift der Vergleichswohnung (Straße, Hausnummer,

Stockwerk, Lagebezeichnung im Stockwerk), Name des Mieters, Angabe des Quadratmeterpreises mit Angabe der Gesamtgröße der Wohnung. Die Hausverwaltung teilte mit, dass die Daten des Bürgers in keinem weiteren Schreiben angegeben wurden.

Der TLfDI entgegnete daraufhin, dass gemäß § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Verarbeiten ist gem. § 3 Abs. 4 BDSG auch das Übermitteln personenbezogener Daten in der Weise, dass die Daten an einen Dritten weitergegeben werden. Der § 558a Abs. 2 Nr. 4 BGB ist für sich isoliert keine hinreichende Rechtsgrundlage dahingehend, vollständige Namen von Mietparteien der Vergleichsobjekte oder sonstige Informationen hierzu an andere Mieter übermitteln zu dürfen. *In der Kommentierung zum § 558a BGB nach Palandt, Rn. 11 heißt es dazu, dass die Vergleichswohnungen für den Mieter identifizierbar sein müssen, damit diese zugeordnet werden können, um beurteilen zu können, ob der Vergleich angemessen ist. Die Angabe der Adresse, des Geschosses und bei einem Mehrfamilienhaus die genaue Lage im Geschoss, die Wohnungsnummer oder aber auch den Namen des Mieters sowie die Quadratmeterzahl und -größe genügen an dieser Stelle.*

Dabei ist zu beachten, dass eben auch die sonstigen Informationen, die bei der Angabe einer Vergleichswohnung notwendig sind, personenbeziehbare Informationen sind, die einer natürlichen Person, dem Mieter, zugeordnet werden können. Rechtsgrundlage für eine Weitergabe dieser weiteren Informationen kann jedoch § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein. Das Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, Begründung einer Mieterhöhung, ist gemäß § 28 Abs. 1 Nr. 2 BDSG nur zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle – nämlich die des Vermieters, die Mieterhöhung rechtmäßig durchzusetzen – erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Bei der Abwägung dieser Interessen muss zwischen der Übermittlung des Namens und den sonstigen Identifizierungsmerkmalen der Wohnung unterschieden werden.

Die Weitergabe der Identifizierungsmerkmale der Vergleichswohnungen wie Adresse, Geschoss, Lage im Geschoss bzw. Wohnungsnummer kann gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt sein. Berechtigtes Interesse des Vermieters ist dabei, sein Mieterhöhungsverlangen auf eine Art und Weise zu begründen, mit der es vor Gericht Bestand haben kann. Eine der vom Gesetzgeber eingeräumten Möglichkeiten ist dabei das Vorlegen von drei Vergleichswohnungen. Das Interesse des Vermieters umfasst daher auch, diese so genau zu beschreiben, dass die Begründung wirksam ist.

Eben diese Angaben, die hierfür notwendig sind, nämlich Art, Größe, Preis und Lage der Wohnung, betreffen aber auch die unmittelbare Privatsphäre des jeweiligen Mieters. Es handelt sich dabei, wie oben bereits erwähnt, um personenbeziehbare Daten. Auch der Mieter hat ein schützenswertes Interesse an der Geheimhaltung dieser wirklich sehr privaten Informationen. Im Rahmen der nunmehr notwendigen Interessenabwägung hat man diese widerstreitenden Interessen gegeneinander abzuwägen. Weil die gesetzliche Wertung des § 558a BGB dabei Beachtung finden muss, ist in der Regel davon auszugehen, dass die schutzwürdigen Interessen des jeweiligen Mieters nicht überwiegen. Um dies bewerten zu können, müssen die jeweiligen Mieter der Wohnungen allerdings vorab befragt werden, ob aus deren Sicht irgendwelche schutzwürdigen Interessen bestehen. Anders ist die Nennung des Vor- und Nachnamens des jeweiligen Mieters der Vergleichswohnung zu bewerten. Hier überwiegt das schutzwürdige Interesse des Mieters an dem Ausschluss der Verarbeitung oder Nutzung zumindest hinsichtlich seines Vor- und Nachnamens zum Zwecke der Angabe von Vergleichswohnungen im Rahmen des § 558a Abs. 2 Nr. 4 BGB gegenüber der Wahrung berechtigter Interessen der Hausverwaltung an der Erfüllung der Geschäftszwecke, hier dem Erfordernis aus § 558a Abs. 2 Nr. 4 BGB, der Angabe von Vergleichsobjekten nachzukommen. Der Mieter hat ein schutzwürdiges Interesse daran, dass seine Daten, so hier insbesondere die Angabe seines Namens in Schreiben, welche an andere Mieter gerichtet sind, durch den Vermieter geschützt werden und er anonym bleiben kann. Weil es hier an der im Rahmen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG notwendigen Erforderlichkeit der Übermittlung des Namens fehlt, hätte es einer Einwilligung des betroffenen Mieters bedurft, die den Voraussetzungen des § 4a BDSG entspricht.

Die Hausverwaltung bezog daraufhin Stellung. Der Hausverwaltung sei die Problematik des Schutzes der persönlichen Daten des Mieters auf der einen Seite und der Wahrung der Interessen des Vermieters für die Erhöhung der Miete auf der anderen Seite durchaus bewusst. Allerdings sei die Hausverwaltung bisher davon ausgegangen, dass die Vergleichswohnungen so genau wie möglich beschrieben werden müssen, um den Mieter in die Lage zu versetzen, genau zu prüfen, um welche Vergleichswohnungen es sich handelt und ob das Erhöhungsverlangen des Vermieters gerechtfertigt ist. Die Hausverwaltung bedankte sich für die Klarstellung und versicherte die rechtlichen Hinweise zukünftig zu beachten.

Gemäß § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Verarbeiten ist gem. § 3 Abs. 4 BDSG auch das Übermitteln personenbezogener Daten in der Weise, dass die Daten an einen Dritten weitergegeben werden. Der § 558a Abs. 2 Nr. 4 BGB ist für sich isoliert keine hinreichende Rechtsgrundlage dahingehend, vollständige Namen von Mietparteien der Vergleichsobjekte oder sonstige Informationen hierzu an andere Mieter übermitteln zu dürfen. Dabei ist zu beachten, dass eben auch die sonstigen Informationen, die bei der Angabe einer Vergleichswohnung notwendig sind, personenbeziehbar sind, die einer natürlichen Person, dem Mieter, zugeordnet werden können.

3.46 Ich bin du, du bist ich?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Unternehmens, dass die Identität dieses Unternehmens gestohlen und die Daten bei angeblichen Verkäufen von Waren genutzt worden seien, um an die Gelder der Käufer zu gelangen. Recherchen ergaben, dass die Adresse des Unternehmens von einem anderen Unternehmen mit einem ähnlich klingenden Namen als Rechnungsadresse genutzt sowie auf der Website unter Kontaktinformationen aufgeführt wurde.

Nach § 1 Bundesdatenschutzgesetz (BDSG) ist der Zweck des Bundesdatenschutzgesetzes, den Einzelnen davor zu schützen, dass er

durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

In dem vorliegenden Fall wurden die Daten eines Unternehmens missbräuchlich verwendet. Somit ist das Unternehmen nicht Betroffener in dem Sinne, da es sich bei einem Unternehmen um eine juristische Person und nicht um eine natürliche Person handelt. Daher musste der TLfDI leider mitteilen, dass er in diesem Fall sachlich nicht zuständig ist. Anders wäre der Sachverhalt zu beurteilen, wenn auch die Daten der Unternehmensangehörigen, wie z. B. der Name, im Rahmen des Identitätsbetrugs genutzt worden wären. Bei diesen Daten handelt es sich wiederum um personenbezogene Daten, da die Daten natürliche Personen betreffen.

§ 3 Abs. 1 BDSG definiert personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Sofern keine Daten, die mit einer natürlichen Person verknüpft werden können (z. B. Namen, Zugehörigkeiten und Funktionen in einem Unternehmen) in einem Identitätsbetrug genutzt werden, sondern es sich lediglich um reine Unternehmensdaten handelt, ist der TLfDI nicht zuständig.

3.47 Geheimnis: Akten einer Steuerberatungskanzlei

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass in einem derzeit nicht mehr gewerblich genutzten Gebäude Akten einer Steuerkanzlei lagern und dieses Gebäude nunmehr von den Eigentümern verkauft wurde.

Der TLfDI wandte sich daraufhin an die Eigentümer und den zuletzt in diesem Gebäude tätigen Steuerberater als möglichen Verantwortlichen und forderte diesen auf, die Akten im Gebäude zu beräumen bzw. fachgerecht zu entsorgen. Daraufhin teilte der Steuerberater dem TLfDI mit, dass es zwar richtig sei, dass er zuletzt in dem Gebäude mit seiner Steuerkanzlei tätig gewesen sei, die Aktenbestände aber wohl zum großen Teil nicht von ihm stammen, sondern noch von seinem Vorgänger, von dem er die Kanzlei seinerzeit übernommen habe. Daraufhin wurde vom TLfDI eine Vor-Ort-Kontrolle der

lagernden Akten durchgeführt. Diese ergab, dass es sich bei den Akten wirklich um solche handelte, die keinen Aufbewahrungsfristen mehr unterliegen und daher der fachgerechten Entsorgung zuzuführen sind. Die Entsorgung von Altaktenbeständen unterliegt datenschutzrechtlich § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG), da es sich um eine Verarbeitung personenbezogener Daten handelt. Diese ist jedoch nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Gemäß § 35 Abs. 2 Nr. 3 sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Aus diesem Grunde wurde auch der Vorinhaber der Kanzlei angeschrieben und aufgefordert, die Altaktenbestände zu entsorgen. Die Beteiligten wurden seitens des TLfDI darauf aufmerksam gemacht, dass bei der datenschutzgerechten Entsorgung der Akten darauf zu achten ist, dass diese nach DIN 66399-2 und der dortigen Sicherheitsstufe P-5 vernichtet werden. Eine Vernichtung unterhalb dieser Sicherheitsstufe würde nicht den datenschutzrechtlichen Vorgaben entsprechen, da es sich vorliegend um Daten handelt, die einem besonderen Schutzbedarf unterfallen. Die dem Steuerberater anvertrauten Geheimnisse unterfallen dem Schutzbereich des § 203 Strafgesetzbuch (StGB). Es ist also darauf zu achten, dass eine Kenntnisnahme durch Dritte deswegen beim Vernichtungsprozess absolut ausgeschlossen ist.

Wird die Vernichtung durch Dritte durchgeführt, ist mit diesem Unternehmen hinsichtlich der Vernichtung ein entsprechender Vertrag über die Auftragsdatenverarbeitung nach § 11 BDSG zu schließen. Nach Aufforderung des TLfDI zur datenschutzgerechten Entsorgung der Altaktenbestände einigten sich die Kanzleihinhaber darüber, die Aktenbestände gemeinschaftlich mithilfe eines zertifizierten Aktenentsorgungsunternehmens zu entsorgen. Die Vorgaben des TLfDI wurden eingehalten und die Entsorgung erfolgreich durchgeführt.

Bei Verlassen eines Firmengebäudes wegen Verkaufs oder Geschäftsaufgabe dürfen keine Aktenbestände zurückgelassen werden. Die Akten müssen archiviert und bei Ablauf der Aufbewahrungsfrist datenschutzgerecht vernichtet werden. Die Entsorgung von Altaktenbeständen unterliegt datenschutzrechtlich § 4 Abs. 1 BDSG, da es sich um eine Verarbeitung personenbezogener Daten handelt. Diese ist jedoch nur zulässig, wenn das BDSG oder eine andere

Rechtsvorschrift dies erlaubt oder anordnet. Gemäß § 35 Abs. 2 Nr. 3 sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Handelt es sich bei dem Aktenmaterial um Geheimnisse i. S. v. § 203 StGB, muss eine Kenntnismahme durch unbefugte Dritte beim Vernichtungsprozess ausgeschlossen sein.

3.48 TLfDI kontrolliert Weihnachtsmann ;-)

In der Vorweihnachtszeit wollte ein engagierter Bürger wissen, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das Weihnachtspostamt der Deutschen Post AG geprüft habe. Namentlich war die Adresse „An den Weihnachtsmann in 99706 Himmelsberg“ angegeben. Sollte eine Prüfung nicht erfolgt sein, bat er dies – aufgrund des zu erwartenden hohen Andrangs – nachzuholen.

Das Bundesdatenschutzgesetz (BDSG) ist dem Grunde nach § 1 Abs. 2 Nr. 3 anwendbar, sofern es sich beim Weihnachtsmann um eine Stelle handelt, die nicht in einem anderen Mitgliedsstaat der europäischen Union (EU) oder im europäischen Wirtschaftsraum (EWR) ihren Sitz hat, § 1 Abs. 5 Satz 1 BDSG. Der Sitz des Weihnachtsmannes und damit auch Ort der Datenverarbeitung sind strittig. Vertreten werden hauptsächlich die Länder Schweden und Finnland, sowie Grönland und der Nordpol. Jedenfalls hat der Weihnachtsmann keinen Sitz in Deutschland. Dies kann festgestellt werden, da er aufgrund der Art und des Umfangs seiner Tätigkeit als sogenannter Istkaufmann nach § 1 Abs. 1 Handelsgesetzbuch (HGB) im Handelsregister eingetragen sein müsste. Da es an einer solchen Eintragung fehlt und dem Weihnachtsmann grundsätzlich Rechtstreue unterstellt werden kann, ist also davon auszugehen, dass ein Sitz in Deutschland nicht existiert. Je nach tatsächlichem Sitz des Weihnachtsmanns würde eine Zuständigkeit des TLfDI schon aufgrund von § 1 Abs. 5 Satz 1 BDSG ausscheiden. Beim Sitz in Grönland oder gar am Nordpol hingegen könnte der TLfDI nach § 1 Abs. 5 Satz 1 BDSG zuständig sein, da dann eine Stelle, die ihren Sitz nicht innerhalb der EU oder des EWR hat, die Datenerhebung und -verarbeitung im (u. a.) Thüringer Inland durchführt.

Die Frage des tatsächlichen Sitzes des Weihnachtsmannes kann aber dahinstehen. Beim Weihnachtsmann handelt es sich, ebenso wie

beim Konkurrenzunternehmen Christkind, höchstwahrscheinlich um eine Angelegenheit der Religionsausübung, bzw. um das Innehaben und Ausüben einer religionsspezifischen Funktion, jedenfalls aber um eine andere vergleichbare organisationsinterne Angelegenheit der Religionsgesellschaft. Damit handelt es sich um den Kernbereich der durch Art. 137 Weimarer Reichsverfassung geschützten Autonomie der Religionsgesellschaften, weswegen der TLfDI nicht zuständig ist (vgl. auch Dammann in Simitis, 8. Auflage, § 2, Rn. 113). Zuständig wäre in diesem Fall je nach persönlicher Einstellung der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland, Böttcherstraße 7, 30419 Hannover oder der Diözesandatenschutzbeauftragte, Chausseestraße 1, 39218 Schönebeck.

Für sein unterstützendes Organ, nämlich das Weihnachtspostamt unter der Adresse „An den Weihnachtsmann, 99706 Himmelsberg“, betrieben durch die Deutsche Post AG, besteht leider beim TLfDI ebenfalls keine Zuständigkeit. Nach § 42 Abs. 3 Postgesetz ist hierfür die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig.

Bedauerlicherweise war es dem TLfDI nicht möglich, weder den Weihnachtsmann selbst, noch das benannte Postamt zu kontrollieren.

In Angelegenheiten der Religionsausübung der beiden christlichen Kirchen bzw. bei organisationsinternen Angelegenheiten der Religionsgesellschaften ist der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland oder der Diözesandatenschutzbeauftragte zuständig. Hinsichtlich des unterstützenden Organs des Weihnachtsmannes, nämlich das Weihnachtspostamt, betrieben durch die Deutsche Post AG, besteht beim TLfDI leider keine Zuständigkeit. Hierfür ist nach § 42 Abs. 3 Postgesetz die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig.



© Spencer – 3D Man Office / Fotolia.com

4 Datenschutzkonformität von unternehmensinternen Unterlagen

4.1 Datenschutz auch bei Korruptionsbekämpfung

In einem Thüringer Unternehmen wurde eine neue Dienstanweisung mit dem Thema Korruptionsprävention und -bekämpfung herausgegeben. Der Betriebsratsvorsitzende des Unternehmens wandte sich mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). In der Dienstanweisung war eine Regelung enthalten, nach der die Mitarbeiter des Unternehmens mitteilen sollten, welche Firmen, mit denen das Unternehmen in Geschäftsverbindung stand, diese auch privat beauftragen wollen. Dies sollten sie ihrem direkten Vorgesetzten

oder der Geschäftsführung anzeigen. Der Betriebsratsvorsitzende war der Auffassung, dass es völlige Privatsache sei, von wem ein Mitarbeiter bzw. dessen Familie Ware und Dienstleistungen bestellt, bezieht oder kauft.

Der TLfDI erfragte bei dem Unternehmen die Rechtsgrundlage dieser Regelung in der neuen Dienstanweisung. Das Unternehmen teilte mit, dass das vorgesehene Vorgehen dem Schutz der Betroffenen diene. Es solle vermieden werden, dass Sonderkonditionen, die mit bestimmten Unternehmen vereinbart werden, auch bei Vertragsbeziehungen mit der Privatperson zum Einsatz kommen bzw., dass eventuell ein Verdacht in dieser Hinsicht entsteht.

Da es sich um ein Unternehmen in 100 prozentiger kommunaler Trägerschaft handelte, war zunächst zu klären, ob das Thüringer Datenschutzgesetz (ThürDSG) oder das Bundesdatenschutzgesetz (BDSG) gilt. Das Unternehmen legte auf Nachfrage des TLfDI dar, dass es als juristische Person am Wettbewerb teilnehme. Damit ist nach § 26 ThürDSG nur der Fünfte Abschnitt des ThürDSG, ausgenommen § 34 Abs. 2 ThürDSG, und ansonsten das BDSG mit Ausnahme des 2. Abschnitts und des § 38 BDSG anwendbar. Das bedeutet, dass grundsätzlich alle Bestimmungen des BDSG auf dieses kommunale Wettbewerbsunternehmen anwendbar sind, mit Ausnahme der Bestimmungen, die die Datenschutzaufsicht betreffen. Diese richtet sich nach den für öffentliche Stellen geltenden Vorschriften des ThürDSG.

Zur Regelung in der Dienstvereinbarung merkte der TLfDI Folgendes an:

Nach der Definition des § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelheiten über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Daher stellt die Anzeige, dass ein bestimmter Mitarbeiter beabsichtigt, ein bestimmtes Unternehmen im privaten Bereich zu beauftragen, selbstverständlich eine Erhebung personenbezogener Daten dar. Der anzuzeigende Sachverhalt bezieht sich jeweils auf einen bestimmten Mitarbeiter. Für die Erhebung, Verarbeitung und Nutzung der Beschäftigten Daten im Zusammenhang mit Korruptionsbekämpfung oder -verhinderung kommt § 32 Abs. 1 Satz 2 BDSG zur Anwendung. Danach können zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im

Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Sollte also ein konkreter Verdacht bestehen, dass besondere Vorteile aus den Geschäftsbeziehungen des Unternehmens mit dem privat zu beauftragenden Unternehmen in Anspruch genommen werden oder werden sollen, ist gegen eine derartige Datenerhebung nichts einzuwenden. Hinsichtlich der Verhältnismäßigkeit ist zu beachten, dass es sich im Regelfall bei privater Beauftragung eines Unternehmens, das auch in Geschäftsbeziehung mit der Beschäftigungsfirma steht, um Geschäfte des täglichen Lebens handelt. Daher wäre nur dann eine mögliche Datenerhebung begründet, wenn es sich um einen nicht unerheblichen Betrag bzw. Auftrag handeln sollte. Bei jeglicher Beauftragung eines Unternehmens bereits zu unterstellen, dass von Beschäftigten Vorteile aus der Geschäftsbeziehung mit dem Arbeitgeber gezogen werden sollen, die im Bereich der Korruption bzw. der persönlichen Vorteilsnahme anzusiedeln wären, geht zu weit.

Der TLfDI sah daher die in Rede stehende Passage der Dienstanweisung als unzulässig an. Nach intensivem Schriftwechsel, in dessen Verlauf dem Unternehmen die Rechtslage dargelegt wurde, passte das Unternehmen die Passage der Dienstvereinbarung den datenschutzrechtlichen Anforderungen des TLfDI an. Von der Meldepflicht wurden nunmehr Geschäfte des täglichen Lebens ausgenommen, und in anderen Fällen wurden die Mitarbeiter angehalten, auch Angebote anderer Firmen einzuholen, um sicherzustellen, dass keine unverhältnismäßig günstigeren Konditionen vereinbart wurden.

Daten über Beschäftigte dürfen auch zum Zweck der Korruptionsbekämpfung und -verhinderung nur erhoben, verarbeitet oder genutzt werden, wenn § 32 BDSG dies zulässt. Da hier eine Straftat verhindert werden soll, kommt § 32 Abs. 1 und 2 BDSG zur Anwendung, nach dem es zu dokumentierende tatsächliche Anhaltspunkte für den Verdacht geben muss, dass der Betroffene im Bestechungsverhältnis eine Straftat begangen hat. Jedes Unternehmen muss daher prüfen, ob die Verhinderung von Korruption auch durch andere Maßnahmen als die Datenerhebung möglich ist.

4.2 Datenschutz im Sportverein – was dürfen SV, FC und Co.?

Ein Sportverein bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darum, die vereinseigene Datenschutzverordnung hinsichtlich ihrer Vereinbarkeit mit dem Bundesdatenschutzgesetz zu überprüfen.

Beim TLfDI wurde das vereinseigene Regelungswerk näher beleuchtet und zunächst konnte festgestellt werden, dass es erfreulicherweise in seinen Grundzügen bereits den gesetzlichen Anforderungen entsprochen hat.

Grundsätzlich dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, soweit eine Vorschrift des Bundesdatenschutzgesetzes (BDSG) oder eine sonstige Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. In § 28 Abs. 1 BDSG findet sich die zentrale Rechtsgrundlage für den Umgang mit personenbezogenen Daten in Vereinen. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1). Die Mitgliedschaft in einem Verein ist als ein solches Schuldverhältnis anzusehen. Nur auf solche Daten, die der Verein zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt, darf der Verein gem. § 28 Abs. 1 Nr. 1 BDSG zugreifen. Der in § 28 BDSG normierte Geschäftszweck ist in Vereinen mit dem Satzungszweck gleichzusetzen. Demnach ist für Vereine nach § 28 Abs. 1 Nr. 1 BDSG das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Satzungszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung der Mitgliedschaft im Verein erforderlich ist. Dies schließt zumeist die Erhebung und Speicherung der Daten hinsichtlich Name, Vorname und Anschrift des Vereinsmitglieds ein.

Kommunikationsdaten werden neben der Anschrift für den Verein nicht unbedingt zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft benötigt. Es muss dem jeweiligen Mitglied selbst überlassen bleiben, ob es Angaben dazu machen möchte oder nicht. Es sollte daher klar im Mitgliedsantrag erkennbar sein, dass es sich bei den Kommunikationsdaten, wie E-Mail-

Adresse oder Telefonnummer, nicht um Pflichtangaben, sondern um freiwillige Angaben handelt. Allgemein muss bei der Frage, welche Mitgliederdaten erforderlich sind, immer der Grundsatz der Datenvermeidung und -sparsamkeit nach § 3a Satz 1 BDSG beachtet werden. Wenn der Verein für Funktionsträger auch Angaben zu Lizenzen und deren Gültigkeit erfasst, kann dies ebenfalls im Hinblick auf die jeweiligen satzungsgemäßen Aufgaben erfolgen. Die Erhebung und Verarbeitung der Bankverbindung ist auch nur zulässig, wenn die Satzung eine Zahlung der Vereinsbeiträge per Bankeinzug vorsieht. Ohne eine entsprechende Verpflichtung durch die Satzung ist der Einzug nicht erforderlich zur Gestaltung der Mitgliedschaft.

In Bezug auf eine mögliche Datenweitergabe an Dritte ist festzustellen, dass im Verein zuständige Personen keine Dritten im Sinne des § 3 Abs. 4 Nr. 3 BDSG sind. Danach ist Dritter jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dies können z. B. Dachverbände sein. Hier handelt es sich um eine Datenübermittlung an Dritte im Sinne der vorgenannten Vorschrift. Folglich benötigt ein Verein, der seine Mitgliederdaten an die Dachorganisationen übermittelt will oder soll, eine Rechtsgrundlage oder die ausdrückliche Einwilligung der betroffenen Mitglieder. Es sollte sich für die jeweiligen Mitglieder aus der Satzung ableiten, welche Daten genau zu den notwendigen personen- und vereinsbezogenen Daten zählen.

Wegen der bestehenden Datenschutzverantwortung in einem Verein ist auch hier für einen ordnungsgemäßen Umgang mit den Mitgliederdaten zu sorgen und es sind technische und organisatorische Maßnahmen im Sinne des § 9 BDSG zu ergreifen. Insbesondere müssen die Daten gegen den Zugriff unberechtigter Dritter geschützt werden. Wird bei der Vereinskommunikation in zulässiger Weise mit einem E-Mail-Verteiler gearbeitet, sollte grundsätzlich der bcc-Modus genutzt werden. Es bedarf auch einer Verpflichtung derjenigen Personen auf das Datengeheimnis, die mit der Verarbeitung von personenbezogenen Daten im Verein betraut sind, vgl. § 5 BDSG. Soweit ehrenamtliche Mitarbeiter im Verein mit der Datenverarbeitung befasst sind, sind auch sie auf das Datengeheimnis zu verpflichten. Dazu sollte der Verein ein Merkblatt vorbereiten und dieses gegenzeichnen lassen.

Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, soweit eine Vorschrift des BDSG oder eine sonstige Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene ein-

gewilligt hat, § 4 Abs. 1 BDSG. § 28 Abs. 1 BDSG ist die zentrale Rechtsgrundlage für den Umgang mit personenbezogenen Daten in Vereinen, da das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung nur als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen, also für die Mitgliedschaft in einem Verein, erforderlich ist. Dabei darf nur auf solche Daten zugegriffen werden, die der Verein zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt. Ein Blick in die jeweilige Vereinssatzung ist daher unerlässlich.

4.3 Da wird der Hund in der Pfanne verrückt

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen eine Eingabe beim Bayerischen Landesamt für Datenschutzaufsicht zugeleitet. Der Eintrag im Vereinsregisterauszug ergab, dass der betroffene Hundeverband e. V. seinen Sitz in Thüringen hat. Der TLfDI wurde als zuständige Stelle um Übernahme des Falles gebeten. Der Verein veröffentlichte regelmäßig bestimmte Vereinsmitglieder samt Adresse in einer Zeitschrift.

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit wandte sich der TLfDI mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Vereinsvorsitzenden. In seiner Bitte um Stellungnahme teilte der TLfDI dem Vereinsvorsitzenden mit, dass er darauf aufmerksam geworden ist, dass personenbezogene Daten, u. a. die genaue Adresse einzelner Mitglieder, in einer Verbandszeitschrift veröffentlicht wurden. Die personenbezogenen Daten wurden zuvor von seinem Verband erhoben und an den Verlag der Zeitschrift übermittelt. Bei der betroffenen Verbandszeitschrift handelte es sich um eine monatlich erscheinende, auch über den Handel zu beziehende Zeitschrift. Daher handelte es sich hierbei nicht um eine reine Mitgliederzeitschrift, vielmehr kann die Zeitschrift grundsätzlich von jedermann gekauft werden. Im Mittelteil einer jeden Ausgabe dieser Zeitschrift werden über mehrere Seiten umfangreich Kontaktdaten von o. g. Personen (Namen mit vollständiger Anschrift und Telefonnummer) veröffentlicht. In der betreffen-

den Ausgabe betraf dies ca. 400 Personen auf 8 1/4 Seiten. Soweit dem TLfDI bekannt geworden war, wurde seitens des Verlags / Herausgebers zu keiner Zeit um eine Zustimmung zur Veröffentlichung der Kontaktdaten gebeten.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Darüber hinaus ist der Betroffene nach § 4 Abs. 3 BDSG von der verantwortlichen Stelle u. a. über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern zu unterrichten.

Der Vereinsvorsitzende führte in seiner Stellungnahme aus, dass nach der Satzung seines Verbandes eine Bezugspflicht des offiziellen Mitteilungsblattes, wie er es nannte, für die Mitglieder bestand. Aus dieser ergab sich auch, dass die Namen von bestimmten Mitgliedern in dem offiziellen Mitteilungsblatt jeweils zu veröffentlichen waren. Dies sei für den Verein wegen der besonderen Tätigkeit dieser Mitglieder wichtig. Auch wurde die Auffassung vertreten, dass es sich bei der Veröffentlichung um ein Presseergebnis handle und der TLfDI damit nicht zuständig sei.

Nach § 41 Abs. 1 BDSG i. V. m. § 11a Thüringer Pressegesetz (TPG) hat das Land Thüringen in seiner Gesetzgebung vorgesehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a BDSG entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 BDSG zur Anwendung kommen. Als Normadressaten gelten daher Unternehmen oder Hilfsunternehmen der Presse. Um die grundrechtlich gewährleistete Pressefreiheit sicherzustellen, ist dabei zunächst von der Begriffsdefinition in Art. 5 Abs. 1 Satz 2 Grundgesetz auszugehen. Daher gilt das BDSG in seinen wesentlichen Teilen nicht, soweit die Datenverarbeitung vom Grundrecht der Pressefreiheit gedeckt ist. Ausgangspunkt ist daher der sogenannte formelle Pressebegriff, wonach die Art und der auf die Verarbeitung gerichtete Zweck, nicht der Inhalt oder die Qualität der Veröffentlichung entscheiden. Danach gehören in diesem formellen Sinn zur Presse alle mittels Buchdruckerpresse oder eines sonstigen zur Massenherstellung geeigneten Vervielfältigungsverfahrens hergestellten und zur Verarbeitung bestimmten Schriften, bespro-

chene Tonträger, bildliche Darstellungen mit und ohne Schrift und Musikalien mit Text oder Erläuterungen (vgl. *Dix* in Simitis, Kommentar zum BDSG, § 41 Rn. 9). Darunter fällt auch dieses offizielle Mitteilungsblatt des Vereins.

Als Unternehmen der Presse einzuordnen sind vor allem Zeitungs-, Zeitschriften und Buchverlage, aber auch selbstständige Journalisten. Dagegen können Presseabteilungen von Wirtschaftsunternehmen, Verbänden, Parteien usw., die Werks-, Kunden- oder Mitgliederzeitschriften herausgeben, nur dann vom Medienprivileg profitieren, wenn sie eine von der übrigen Unternehmensverwaltung abgetrennte Organisationseinheit bilden. Eine solche abgetrennte Organisationseinheit war in diesem Fall der Verlag.

Nach § 41 Abs. 1 BDSG sind aus dem Anwendungsbereich des BDSG jedoch nur diejenigen Datenbestände der Medien, die ausschließlich zu eigenen journalistisch-redaktionellen Zwecken (im Gegensatz zur Veröffentlichung einer bloßen Auflistung von Informationen) verarbeitet oder genutzt werden, weitgehend herausgenommen. Erfasst sind hingegen die personenbezogenen Informationen, die von Journalisten, Redakteuren etc. zu Zwecken der Recherche sowie der Vorbereitung und Herstellung von zur Veröffentlichung bestimmten Artikeln, Sendungen oder sonstigen redaktionellen Texten entweder unmittelbar erhoben oder aus anderen Quellen beschafft werden. Neben einer journalistisch-redaktionellen Tätigkeit verlangt die Veröffentlichung für einen unbestimmten Personenkreis eine gewisse schöpferische, der öffentlichen Meinungsbildung dienende Leistung des Redakteurs, die eine planvolle inhaltliche, sprachliche oder grafische Bearbeitung beinhaltet (s. VGH München, Urteil vom 25. März 2015 – 5 B 14.2164). Eine solche Leistung liegt aber gerade hier in der Veröffentlichung von Mitgliederlisten samt Namen, Adressen und Telefonnummern **nicht** vor. § 41 BDSG und § 11a TPG forderten zudem eine Verarbeitung ausschließlich zu journalistisch-redaktionellen Zwecken.

Daran fehlte es in diesem Fall, weil weder der Vorstand noch eine andere Stelle innerhalb des Vereins oder des Verlags, deren sich der Verein zur Veröffentlichung des Mitteilungsblattes bediente, ausschließlich für die Verarbeitung von Informationen zu journalistisch-redaktionellen Zwecken tätig waren. Vielmehr verfolgte der Verein, wie ein Blick in die Satzung zeigte, die Zwecke des Vereins und nicht eine Tätigkeit im Pressewesen. Das hier vorliegende Vereinshandeln ist auf die Umsetzung der Satzung, insbesondere auf die

Nennung der Namen der Mitglieder, gerichtet, nicht jedoch auf die unternehmerische Tätigkeit der Herausgabe von Druckwerken. Das bloße Veröffentlichen von Information mit der vorgenannten Zielrichtung zu anderen Zwecken macht den Veröffentlichenden auch noch nicht zu einem Unternehmen der Presse. Denn dann müsste man jede politische Partei, jedes Wirtschaftsunternehmen und auch jede Privatperson als Presseunternehmen ansehen, wenn sie sich nur mittels einer Homepage mit Informationen über ihre Aktivitäten an die Allgemeinheit wendet (dazu Gola/Schomerus, BDSG, 12. Aufl. 2015, § 41 Rn. 10a).

Im Ergebnis fehlte es daher an einer Verarbeitung von Daten zu ausschließlich journalistisch-redaktionellen Zwecken. Der Zweck der Veröffentlichung lag in der Umsetzung der Vereinssatzung.

Daher war nach Auffassung des TLfDI das BDSG auch auf die Veröffentlichungen in der Zeitschrift anwendbar. Es bedurfte daher für die Verarbeitung und Nutzung, hier in Form der Veröffentlichung im offiziellen Mitteilungsblatt, der personenbezogenen Daten der Mitglieder einer Rechtsvorschrift, die dies erlaubte oder anordnete, oder der Einwilligung der Betroffenen, § 4 Abs. 1 BDSG. Seitens der von der Veröffentlichung betroffenen Mitglieder lagen keine solchen Einwilligungen in die Veröffentlichung ihrer personenbezogenen Daten vor.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Speichern und Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Geschäftszweck im Sinne dieser Vorschrift ist dabei jeder Zweck einer privaten Stelle, also jeder Zweck, der sich nicht im ausschließlich persönlichen oder familiären Bereich bewegt. Geschäftszweck im Sinne der Vorschrift ist daher vorliegend der Vereinszweck. Als berechtigtes Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG kommt jedes von der Rechtsordnung gebilligte Interesse infrage. Es genügt jedes Verlangen, das bei vernünftiger Erwägung durch die Sachlage gerechtfertigt ist. Ein solches berechtigtes Interesse hatte der Vereinsvorsitzende nicht vorgetragen.

Selbst wenn man ein solches berechtigtes Interesse angenommen hätte, hätte dieses im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch erforderlich sein müssen. Erforderlich ist eine Datenverarbeitung

dann, wenn sie notwendig für die Erreichung der berechtigten Interessen ist. Es sprach Vieles dafür, dass es hier an der Erforderlichkeit der vorgenommenen Nutzung und Verarbeitung der personenbezogenen Daten der einzelnen Mitglieder fehlte. Es war nicht erkennbar, zu welchem Zweck und aus welchem Grund diese Personen mit Namen, Adressen und Telefonnummern in einem frei zugänglichen Papier veröffentlicht werden sollten. Hier überwogen ganz klar die Interessen der Betroffenen des Vereins.

Ein berechtigtes Interesse des Vereins daran, neben den Namen der Mitglieder noch deren Adressen und Telefonnummern konkret zu benennen, war auch nicht erkennbar.

Der TLfDI erwog als zuständige Aufsichtsbehörde, gegen den Hundeverband e. V. eine Anordnung zu erlassen, die zum Ziel hatte, die mit dem BDSG nicht zu vereinbarende Veröffentlichung bzw. Übermittlung der Mitgliederliste, wie der Verein sie zu dieser Zeit praktizierte, zu unterbinden.

Der Verein passte seine Satzung dementsprechend an. Mit der Änderung der Satzung und deren Umsetzung in die Praxis erachtete der TLfDI das Verwaltungsverfahren für erledigt. Eine Veröffentlichung der Adressen und Telefonnummern wird nach den vorliegenden Informationen in der Zukunft unterbleiben. Es werden nunmehr nur der Name und eine dazugehörige Mitgliedsnummer veröffentlicht. Dies hielt der TLfDI unter Bezugnahme auf die Satzung der verantwortlichen Stelle für datenschutzrechtlich zulässig.

Das „Medienprivileg“, also die weitestgehende Nichtanwendbarkeit des BDSG auf Presseprodukte, gilt nur, soweit dabei ausschließlich redaktionelle oder journalistische Zwecke verfolgt werden. Sobald weitere Zwecke hinzukommen, ist das BDSG anwendbar.

4.4 Falscher Adressat TLfDI

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine schriftliche Anfrage eines Postzustellungsunternehmens. Das Unternehmen hat als Produkt eine sogenannte digitale Poststelle angeboten. So war es für die Kunden möglich, die gesamte Postausgangspost über den Anbieter in digitaler Form laufen zu lassen. Da dem Kundenstamm mehrere öffentliche Stellen nach dem § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) angehörten, erkundigte sich das Unterneh-

men beim TLfDI, ob der TLfDI für datenschutzrechtliche Freigabeverfahren zuständig ist.

Beim erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf es hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung der vorherigen schriftlichen Freigabe durch die Stelle, die den Datenschutz sicherzustellen hat, § 34 Abs. 2 ThürDSG. Diese Stellen sind jedoch nach § 34 Abs. 1 ThürDSG das zuständige Landesministerium, die Gemeinden und Gemeindeverbände oder sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts. Über ein automatisiertes Abrufverfahren gem. § 7 Abs. 1 ThürDSG, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, und über regelmäßige Datenübermittlungen gem. § 7 Abs. 7 ThürDSG ist nach § 7 Abs. 3 ThürDSG der Landesbeauftragte für den Datenschutz unter Mitteilung der Regelungen nach § 7 Abs. 2 ThürDSG vorher zu unterrichten. Ungeachtet der Tatsache, ob es sich bei den Postdienstleistungsunternehmen um ein automatisiertes Abrufverfahren oder eine regelmäßige Datenübermittlung handelt, kann eine Prüfung durch den TLfDI nur dann erfolgen, wenn dies im konkreten Anwendungsfall mit den notwendigen Angaben, hier im Rahmen einer Unterrichtung, vorgelegt wird. Das Unternehmen hatte sich nicht weiter an den TLfDI gewandt. Im Übrigen wäre der TLfDI auch nicht – wie oben dargestellt – für einen Antrag des Freigabeverfahrens vom Postzustellungsunternehmen zuständig gewesen. Somit war das Verfahren seitens des TLfDI beendet.

Eine pauschale Vorabegutachtung einzelner Produkte des Unternehmens, losgelöst von einem Anwendungsfall, kann seitens des TLfDI nicht erfolgen, da auch das Freigabeverfahren an sich nicht vom TLfDI, sondern wie schon beschrieben von den zuständigen Stellen für die Sicherstellung des Datenschutzes durchgeführt wird und der TLfDI in diesem Zusammenhang nur davon unterrichtet wird und ggf. Hinweise erteilt.

4.5 Datenschutz bei der App-Entwicklung

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass ein Thüringer Unternehmen mit der Erstellung einer bundesweit eingesetzten sog. App (application software oder auch Anwendungs-

software, häufig im Bereich mobiler Betriebssysteme zu finden) beauftragt wurde, mithilfe derer eine Vielzahl von personenbezogenen Daten erhoben werden könne und diese Daten danach in einer Datenbank gespeichert und auch für verschiedene Anwendungsmöglichkeiten verarbeitet würden. Da durch den Einsatz einer App potenziell eine Vielzahl von Bürgern betroffen sein kann, war dem TLfDI daran gelegen, die genaue Funktionsweise dieser App zu hinterfragen und sicherzustellen, dass sie den datenschutzrechtlichen Anforderungen genügt. Dazu wurde ein Vor-Ort-Termin mit dem entwickelnden Unternehmen vereinbart und die Funktionsweise und Anwendungsmöglichkeiten vor Ort in Augenschein genommen sowie die technischen und organisatorischen Gegebenheiten genau erörtert. Ergänzend dazu wurde durch den TLfDI auch Kontakt zu den weiteren App-Verwendern aufgenommen und auch die Verwender ähnlicher Apps um Auskunft darüber gebeten. Die technischen Abläufe der Datenerhebung und -speicherung sowie die vertraglichen Grundlagen für diese Datenverarbeitungen werden durch den TLfDI derzeit geprüft und ausgewertet. Da aufgrund der komplexen Struktur der Datenverarbeitung noch Rückfragen beim Entwickler notwendig gewesen sind, liegt ein abschließendes Ergebnis der Prüfung noch nicht vor.

Gerade bei der flächendeckenden Nutzung von Anwendungssoftware besteht die Gefahr, dass es eine Vielzahl von Betroffenen gäbe, wenn diese Software datenschutzrechtliche Mängel aufweisen würde. Aus diesem Grund ist der TLfDI bestrebt, die technische Umsetzung derartiger Software-Lösungen direkt beim Entwickler zu hinterfragen und ggf. Nachbesserungen in der Umsetzung herbeizuführen.



Geschützte Daten – momius – fotolia.com

5 Meldungen nach § 42a

5.1 Leaks

Datenlecks, Datenpannen oder Datendiebstähle müssen unter bestimmten Voraussetzungen der zuständigen Aufsichtsbehörde, sprich: für Thüringen dem Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), sowie dem/den Betroffenen gemeldet werden.

Die Meldepflicht entsteht gemäß § 42a Bundesdatenschutzgesetz (BDSG), wenn bei der verantwortlichen Stelle gespeicherte, besonders sensitive Arten von Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Zu den besonders sensitiven Arten von Daten gehören nachfolgende Datenkategorien:

1. besondere Arten personenbezogener Daten, hierunter fallen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (siehe § 3 Abs. 9 BDSG),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen und
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Jedoch greift die Pflicht nur, wenn für die Rechte oder schutzwürdigen Interessen der Betroffenen schwerwiegende Beeinträchtigungen drohen. Die verantwortliche Stelle muss eine Gefahrenprognose vornehmen. Dabei sind mögliche Folgen der Datenpanne zu identifizieren und im Hinblick auf die möglicherweise eintretenden Belastungen für den Betroffenen zu bewerten. Hierbei darf aber kein zu enger Maßstab angelegt werden, da bei den oben genannten Datenkategorien schon gute Gründe gegen eine solche schwerwiegende Beeinträchtigung vorliegen müssen. Der § 42a BDSG fordert weder erhebliche materielle Schäden noch erhebliche soziale Nachteile. Die Wahrscheinlichkeit, dass Daten veröffentlicht oder kriminell genutzt werden, reicht schon aus. Im Zweifel sollte die verantwortliche Stelle von einer Meldepflicht ausgehen.

Sofern ein solcher Schaden bereits vorgefallen ist, muss keine Abwägung mehr vorgenommen werden.

Die zuständige Aufsichtsbehörde ist unverzüglich über solch einen Vorfall zu informieren. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird.

Um den Unternehmen die Einschätzung zu vereinfachen, hat der TLfDI eine Checkliste entwickelt. Diese ist auf der Homepage des TLfDI

https://www.tlfdi.de/mam/tlfdi/info/checkliste_42bdsgneu.pdf unter

zu finden.



Unter den im Berichtszeitraum gemeldeten Vorfällen findet sich beispielhaft Folgendes: die Entwendung von externen Sicherungsfestplatten bei einem Einbruch in eine Arztpraxis und eine Vermisstenmeldung eines Speichermediums für Ultraschallbilder.

Problematisch war auch, dass Mitarbeiter

Unterlagen an ihre private E-Mail-Adressen verschickten, z. B. Unterlagen zu einem Kreditkartenantrag oder interne Bankgeschäftsunterlagen mit Dateianhängen (inkl. Kundendaten).

In einer weiteren Meldung wurde angezeigt, dass ein Mitarbeiter versehentlich ein ausgefülltes Formular namens „Selbstauskunft“ an einen anderen Kunden versendet hatte.

Darüber hinaus gab es eine Meldung, dass ein Überweisungsbriefkasten einer Bank aufgebrochen wurde.

Besonders prekär war die Veröffentlichung von sehr privaten Daten eines Kunden eines Berufsgeheimnisträgers auf der privaten Facebookseite einer Mitarbeiterin. Sie hatte die Informationen im Rahmen ihrer Tätigkeit aufgeschnappt und dann sofort in ihrem „Facebook-Freundeskreis“ verbreitet.

§ 42a BDSG verpflichtet nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen, den TLfDI und die Betroffenen unverzüglich darüber zu informieren, wenn entsprechend sensible Daten (z. B. Gesundheitsdaten, Konto- und Kreditkarteninformationen) Dritten unrechtmäßig zur Kenntnis gelangt sind (z. B. durch einen Hackerangriff oder einen Diebstahl). Hierbei reicht es, wenn tatsächliche Anhaltspunkte vorliegen, dass unbefugte Dritte mit hoher Wahrscheinlichkeit Kenntnis von den Daten nehmen konnten. Die Meldung muss immer die Art der betroffenen Daten und die Erklärung des Vorfalls, warum die Daten abhandengekommen sind, enthalten. Dem Betroffenen müssen zudem Hilfestellungen aufgezeigt werden. Die Aufsichtsbehörde erhält zusätzlich eine Einschätzung zu den nachteiligen Folgen der unrechtmäßigen Kenntnisnahme und eine Nennung der bisher getroffenen Maßnahmen zur Verhinderung oder Minderung der Folgen (siehe auch o. g. Checkliste). Wer der gesetzlichen Verpflichtung nicht oder nicht rechtzeitig nachkommt, dem droht ein Bußgeld von bis zu 300.000 Euro gemäß § 43 Abs. 2 Nr. 7 BDSG.



Security Camera, CCTV on location, airport - ©alice_photo / Fotolia.com

6 Videoüberwachung

6.1 „1984“ war gestern!

George Orwell würde sich freuen. Vielleicht auch nicht. Nach kurzem Überlegen: Nein, er wäre vermutlich begeistert ob der technologischen Möglichkeiten und entsetzt über das Ausmaß der Überwachung in unserer heutigen Gesellschaft.

Denn: Die technologischen Möglichkeiten zur Überwachung sind weit über das hinausgewachsen, was in seinem ohnehin schon ausreichend beängstigendem Roman „1984“ möglich ist. Viele haben inzwischen Handys, die auf Befehl zuhören und das Gesagte zur Spracherkennung an irgendwelche Server senden, kleine Geräte, die im Wohnzimmer oder Schlafzimmer stehen und auf Zuruf neue Tabs für die Spülmaschine bestellen, allen voran die Videoüberwachung.

Videoüberwachung hat massiv zugenommen. Auch hier im Freistaat Thüringen. Teilweise wird diese von der Bevölkerung sogar begrüßt. Unterhält man sich mit Menschen, bekommt man in der Regel zu hören, es wäre schön, wenn jemand eingreifen könne, sobald etwas passiert. Ein möglicherweise schwerwiegender Irrtum. Nur ein verschwindend geringer Anteil von Videoüberwachungsanlagen ist technisch so ausgestaltet, dass es überhaupt möglich ist, das Gesche-

hen live zu beobachten. Noch ein viel geringerer Anteil dieser Anlagen ist mit jemandem besetzt, der tatsächlich zuschaut oder gar für Hilfe sorgt.

Tatsächlich zeichnen die Videoanlagen nur auf. Alles. Jeden Streit, jeden Kuss, jedes Popeln in der Nase. Eine präzisere Erfassung des menschlichen Verhaltens als das der Videoaufnahme ist kaum möglich. Eingreifen, wenn tatsächlich mal was passiert? Fehlanzeige. Zugegeben, die Aufklärung wird einfacher. Aber ist das Grund genug, um massenhaft Menschen, die sich anstandslos innerhalb der Gesellschaft bewegen, aufzuzeichnen? Dafür gibt es ein Wort: Vorratsdatenspeicherung. In anderem Zusammenhang wurde diese vom Europäischen Gerichtshof bereits mehrmals als rechtswidrig befunden. Trotz mehrerer Anläufe der Bundesregierung, diese umzusetzen. Und auch bei der Videoüberwachung ist im Zuge des internationalen Terrors der Versuch unternommen worden, Freiheitsrechte einzuschränken.

Zum datenschutzrechtlichen Problem wurde die Videoüberwachung erst, als die Technik günstig wurde. Inzwischen sind kleine Anlagen beim Discounter erhältlich. Eine Information über die rechtlichen Voraussetzungen der Videoüberwachung ist dort aber nicht inklusive.

Tatsächlich war die Videoüberwachung, wie auch in den vergangenen Berichtszeiträumen, eines der Schwerpunktthemen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Alleine schon wegen der schieren Masse an rechtswidrigen Überwachungen. Der Gesetzgeber hat die Videoüberwachung nämlich an enge Voraussetzungen gebunden, die ein Betreiber von Videoüberwachungsanlagen eigenständig prüfen muss. Insbesondere sind Verfahren zur biometrischen Gesichtserkennung nur unter sehr engen Voraussetzungen zulässig und beim Einsatz von Videoüberwachungen von Privaten überwiegend nicht erforderlich. Zudem besteht hinsichtlich einer Videoüberwachung von nicht-öffentlichen Stellen eine Meldepflicht gemäß § 4d Abs. 1 BDSG (Urteil des VG Saarland vom 18. Mai 2016, Az. 1 K 63/15, nunmehr bestätigt durch Urteil des OVG Saarlouis vom 14. September 2017). Nur wenn die entsprechenden Voraussetzungen erfüllt sind, darf eine solche Anlage rechtmäßig genutzt werden. Sind die Voraussetzungen nicht erfüllt, droht hingegen ein Bußgeldverfahren. Nach derzeitigem Recht mit einer maximalen Bußgeldhöhe von 300.000 Euro.

Ab Ende Mai 2018, mit Geltung der Datenschutz-Grundverordnung erhöht sich dieses Bußgeld für rechtswidrige Datenerhebung auf maximal 20 Millionen Euro.

Auf den folgenden Seiten berichtet der TLfDI von einigen Fällen, die er im Berichtszeitraum geprüft hat.

6.2 Meldungen nicht nur von Wildkameras

In diesem Fall meldete ein privater Jäger das Betreiben einer Wildtierkamera in seinem eigenen Waldstück zum Verfahrensregister des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an. Seit dem Urteil des *Verwaltungsgerichts Saarland vom 18. Mai 2016, Az.: 1 K 63/15* gilt für die private Jägerschaft und letztlich auch für alle nicht-öffentlichen Stellen, dass auch Wildtierkameras der Meldepflicht des § 4d Bundesdatenschutzgesetz (BDSG) unterliegen. Nach § 4d Abs. 1 BDSG sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe von § 4e BDSG zu melden. Kameras, die Bilder oder Videoaufnahmen aufzeichnen und abspeichern, stellen eine solche automatisierte Datenverarbeitungsanlage dar, die personenbezogene Daten erhebt und meist zugleich verarbeitet, wenn die Aufnahmen gespeichert werden. Ausnahmen für die Meldepflicht bestehen nach § 4d Abs. 2 und 3 BDSG, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Darüber hinaus entfällt die Meldepflicht, wenn die verantwortliche Stelle personenbezogene Daten für sich erhebt, verarbeitet oder nutzt und dabei nicht mehr als neun Personen mit der Datenerhebung- bzw. -verarbeitung beschäftigt sind und eine Einwilligung der Betroffenen vorliegt oder die Datenerhebung für die Vertragsbegründung oder -durchführung erforderlich ist. Somit unterliegen **alle Videoüberwachungsanlagen von nicht-öffentlichen Stellen**, worunter natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts fallen (§ 2 Abs. 4 BDSG), **der Meldepflicht**, sofern kein Ausnahmetatbestand des § 4d BDSG eingreift, was bei einer Videoüberwachung zumeist nicht der Fall ist. Der Verantwortliche hat die von ihm betriebene Videoüberwachung vor der Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden. Örtlich zuständig ist die Aufsichtsbehörde, in der die verantwortliche Stelle ihren Hauptgeschäftssitz hat. In Thüringen ist nach § 42

Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 BDSG der Landesbeauftragte für den Datenschutz sachlich zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich. Zu melden sind nach § 4e Satz 2 i. V. m. § 4d BDSG auch Veränderungen und Beendigungen von bestehenden Verfahren. Grundsätzlich gibt es keine Formvorschrift für die abzugebende Meldung, jedoch hat sich in der Praxis die Schriftform durchgesetzt, d. h. mittels Schreibens oder entsprechenden Formulars. Der Inhalt dieser Meldung ergibt sich aus § 4e Satz 1 BDSG. Dort werden sämtliche erforderlichen Angaben aufgeführt. Der TLfDI hat auf seiner Homepage entsprechende Formulare, sowie Ausfüllhinweise für die verantwortlichen Stellen zur Verfügung gestellt: (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v_.pdf, https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_ausfuellhinweise_zum_meldeformular.pdf).

Die anschließende Aufnahme in das sog. Verfahrensregister bedeutet jedoch nicht, dass die Aufsichtsbehörde die Datenverarbeitung für zulässig erachtet. Es wird bei der Aufnahme lediglich die Vollständigkeit der Angaben überprüft. Die Aufsichtsbehörde ist durch die Meldung nicht gezwungen, diese auch auf die Rechtmäßigkeit der Datenverarbeitung hin zu überprüfen. Nach § 38 Abs. 2 BDSG ist sie lediglich verpflichtet, ordnungsgemäße Verfahren in das Verfahrensregister aufzunehmen. Im Umkehrschluss bedeutet dies aber auch, dass offensichtlich gegen die Datenschutzvorschriften verstoßende Datenverarbeitungen nicht in das Verfahrensregister aufzunehmen sind. Der TLfDI weist hier auch darauf hin, dass es sich bei einer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemachten Meldung um einen Bußgeldtatbestand nach § 43 Abs. 1 Nr. 1 BDSG handelt. Hier kann der TLfDI ein Bußgeldverfahren einleiten.



Grundsätzlich sind von nicht-öffentlichen Stellen sämtliche automatisierte Datenverarbeitungen dem TLfDI zu melden, sofern die verantwortlichen Stellen ihren Hauptgeschäftssitz oder Wohnsitz in Thüringen haben und kein Ausnahmetatbestand nach § 4d Abs. 2 und 3 BDSG eingreift. Zu beachten ist insbesondere, dass die Meldung vor der Inbetriebnahme der Datenverarbeitungsanlage erfolgen

muss. Eine spätere Meldung kann ein Bußgeldverfahren nach sich ziehen. Der Inhalt der erforderlichen Angaben für die Meldung ergibt sich aus § 4e Satz 1 BDSG. Der TLfDI hat auf seiner Homepage entsprechende Formulare, sowie Ausfüllhinweise für die verantwortlichen Stellen zur Verfügung gestellt: (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v_.pdf, https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_ausf_lhinweise_zum_meldeformular.pdf).



6.3 Selbstbedienungsladen ohne Personal, aber mit problematischer Überwachungstechnik?

In Schweden gibt es ein Geschäftsmodell für den ländlichen Raum, das ohne Personal auskommt. Auch ohne Kassen. Kunden müssen sich lediglich registrieren lassen und eine App herunterladen. Über einen Fingerwisch und eine entsprechende Automatik öffnet sich dann die Tür. Die gekaufte Ware müssen die Kunden mit der Handykamera einscannen, gezahlt wird einmal im Monat per Handy-App oder mit EC-Karte. Würde das Konzept auch in Deutschland funktionieren? Ein Unternehmen aus Niedersachsen ist sich da ziemlich sicher. Vorreiter soll Thüringen mit 250 geplanten Standorten sein. Die beschriebenen Selbstbedienungsläden sollen 24 Stunden und sieben Tage die Woche betrieben werden. Aber: Wie schützt sich der Ladenbesitzer gegen unehrliche Kunden? Tatsächlich ist das offenbar ein schwieriges Thema. Die Antwort fängt beim Sortiment an: Das Geschäft führt keine besonders diebstahlgefährdeten Waren wie Zigaretten, Alkohol und Medikamente. Und sie hört bei der Videoüberwachung auf. Geplant waren zehn Kameras im Innen- und zwei Kameras im Außenbereich. Mit der Frage, ob diese Videoüberwachung zulässig sei, wandte sich das Unternehmen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(TLfDI) als Datenschutzaufsicht für den privaten Bereich in Thüringen. Allerdings ist die Zuständigkeit des TLfDI noch nicht eindeutig feststehend. Das geplante Modell sollte zunächst in Thüringen ausgerollt werden. Es war jedoch noch nicht klar, welches Unternehmen sich in das Modell einkaufen und daher dann verantwortliche Stelle sein würde. Nur wenn die Videoüberwachung durch eine Stelle in Thüringen eigenverantwortlich durchgeführt wird, besteht eine Zuständigkeit des TLfDI für die datenschutzrechtliche Bewertung.

Der TLfDI überreichte daher zuerst einmal die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises. Sie enthält die Anforderungen, die alle Aufsichtsbehörden in Deutschland an eine zulässige Videoüberwachung stellen und ist auch auf der Homepage des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf veröffentlicht.

Sofern der TLfDI unter Berücksichtigung des oben Gesagten für die datenschutzrechtliche Beurteilung zuständig sein sollte, stellte sich die Situation nach den bislang vorliegenden Informationen wie folgt dar:



Sowohl im Hinblick auf die Videoüberwachung innerhalb der Selbstbedienungsläden als auch in Bezug auf die zwei Kameras am Eingang beurteilt sich die Zulässigkeit nach § 6b Bundesdatenschutzgesetz (BDSG), da es sich um öffentlich zugängliche Bereiche handelt. Der § 6b BDSG beinhaltet, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zwar können in diesem Fall den Laden nur vorher registrierte Kunden betreten, die Registrierung ist aber grundsätzlich für jedermann möglich. Damit handelt es sich um einen öffentlich zugänglichen Raum. Da es zum Geschäftsmodell gehört, dass kein Servicepersonal vor Ort ist und sich die Kunden selbst im Laden bedienen und die Waren auch selbstständig vor Ort mit einer App oder mit EC-Karte bezahlen, besteht ein berechtigtes Interesse des Betreibers daran, dass das Geschäft videoüberwacht wird. So kann nachvollzogen werden, wenn

die Waren nicht bezahlt worden sind oder es kann reagiert werden, wenn es im Laden zu einem Vorkommnis kommt, sei es, dass es einem Kunden schlecht geht oder dass es zu einer Sachbeschädigung kommt. Die Aufnahmen sollen durch eine Servicestelle rund um die Uhr beobachtet werden. Die Erforderlichkeit ist auch für die Videoüberwachung des Eingangsbereiches gegeben, sofern der Erfassungsbereich der Kameras, wie vom zukünftigen Betreiber beabsichtigt, auf einen Bereich von einem Meter vor der Eingangstür beschränkt ist. Auf die Videoüberwachung muss darüber hinaus den Anforderungen des § 6b Abs. 2 BDSG entsprechend hingewiesen werden. Wichtig ist, dass sich auch ein Hinweis auf die verantwortliche Stelle findet.

Weiterhin ist sowohl bei der Datenspeicherung, beim Monitoring als auch bei der Fernwartung eine sichere Transportverschlüsselung entsprechend dem aktuellen Stand der Technik einzusetzen, sofern die Bilder an einer anderen Stelle eingesehen werden sollen.

Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht mehr abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können (vergleiche die Gesetzesbegründung, Bundestagsdrucksache 14/5793, Seite 63). In begründeten Einzelfällen kann eine längere Speicherdauer angenommen werden. Hier ist abzuwarten, ob Zugang zu den Selbstbedienungsläden auch am Wochenende gegeben sein wird.

Bevor die Videoüberwachungsanlage installiert wird, ist der betriebliche Datenschutzbeauftragte verpflichtet, eine Vorabkontrolle nach § 4d Abs. 5 BDSG durchzuführen, da die beabsichtigte Videoüberwachung zweifelsfrei besondere Risiken für die Rechte und Freiheiten der Kunden aufweist, die während des gesamten Einkaufs gefilmt werden. Nach der gesetzlichen Regelung darf ein Unternehmen ein automatisiertes Verfahren, das besondere Risiken für das Grundrecht auf informationelle Selbstbestimmung für den Betroffenen mit sich bringt, nur einsetzen, wenn der betriebliche DSB vorher überprüft hat, ob dieses Verfahren den Anforderungen des BDSG entspricht. Zu weiteren Einzelheiten und Festlegungen wurde empfohlen, sich mit der zuständigen Aufsichtsbehörde in Verbindung zu setzen,

sobald feststeht, welche Stelle für die Videoüberwachung verantwortlich ist. Im Zuge dessen kann auch geprüft werden, ob möglicherweise eine Einwilligung zu der Videoüberwachung im Container über die Allgemeinen Geschäftsbedingungen möglich ist. In die Videoüberwachung im Außenbereich kann nicht wirksam vorab eingewilligt werden, da sich auch Personen dem Container nähern werden, die die näheren Umstände der Videoüberwachung nicht kennen. Für sie ist keine informierte Einwilligung nach § 4a Abs. 1 Satz 2 BDSG möglich.

Eine geplante Videoüberwachung in einem Einkaufscontainer ohne Personal bedarf einer Vorabkontrolle nach § 4d Abs. 5 BDSG durch den betrieblichen Datenschutzbeauftragten der verantwortlichen Stelle. Eine Übersicht über die erforderlichen Prüfungen und Festlegungen bildet die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“.

6.4 Rundumüberwachung einer Wohnungsanlage

Ein Beschwerdeführer wandte sich im Berichtszeitraum wegen einer Videoüberwachungsanlage, welche auf die öffentliche Straße gerichtet war, an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser ermittelte zunächst den Eigentümer des Gebäudes, an dem die Videokameras angebracht waren. Eigentümer war eine thüringische Immobilienverwaltungsgesellschaft, welche dort auch ihre Geschäftsstelle und Mietwohnungen unterhielt. Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen an diese, um den Sachverhalt abschließend zu ermitteln.

An und in dem Gebäude waren insgesamt sechs Videokameras angebracht. Eine Videokamera befand sich im Wartebereich der Geschäftsstelle der Immobilienverwaltungsgesellschaft. Alle weiteren Kameras befanden sich im Außenbereich. Zwei Kameras bildeten den Parkplatzbereich am Haus ab. Eine weitere erfasste den Stellplatz für die Fahrräder und ein Stück des Gartenbereichs. Weiterhin bildete eine Kamera den Eingangsbereich der Geschäftsstelle ab, wobei der Bereich nur einen Meter ab der Hausfassade erfasst wurde. Der restliche Bereich war geschwärzt. Eine weitere war am Eckbereich des Gebäudes angebracht und bildete jeweils die Fassade des Gebäudes ab. Hier war ebenfalls lediglich ein Meter des Gehweges ab der Hauswand erfasst, der Rest wurde ausgeschwärzt. Die Kame-

ras wurden zur Abschreckung und Abwehr von potenziellen Straftätern und Störern, zur Beweissicherung von Straftaten und zur Geltendmachung von Schadenersatzansprüchen installiert. Die Aufnahmen wurden für 72 Stunden auf einem Festplattenrecorder gespeichert.

Aufgrund des Beobachtens mit den Videokameras werden personenbezogene Daten erhoben und mittels Speicherung auf dem Festplattenrecorder gleichzeitig verarbeitet. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zur Zulässigkeit der Videoüberwachung der nicht-öffentlichen Stellen haben die Datenschutzaufsichtsbehörden im Düsseldorfer Kreis eine Orientierungshilfe erarbeitet, welche der TLfDI auch auf seiner Website zur Verfügung stellt

(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf).



Eine Rechtsvorschrift außerhalb des BDSG, welche die hier betriebene Videoüberwachung erlaubt, ist nicht ersichtlich. Auch eine Einwilligung nach § 4a Abs. 1 BDSG scheidet aus.

Die Zulässigkeit der betreffenden Videoüberwachungsanlage beurteilt sich mit Ausnahme der Kamera, welche den Fahrradständer und den Gartenbereich erfasst, vorliegend nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Diese Bereiche sind als öffentlich zugänglich zu betrachten, da diese von jedermann betreten werden können und öffentlichen Raum wie den Gehweg erfassen. Für die Kamera in der Geschäftsstelle ist dies zumindest während der Geschäftszeiten zu bejahen. Danach ist eine Videoüberwachung in öffentlich zugänglichen Räumen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der angegebene Zweck – Abschreckung und Abwehr potenziellerer Straftäter sowie die Beweissicherung zu diesen Straftaten – wird nur dann seitens des TLfDI als berechtigtes Interesse anerkannt, wenn eine tatsächliche Gefahrenlage durch die verantwortliche Stelle

nachgewiesen werden kann. Dies kann durch Dokumentation der Vorkommnisse bzw. Nennung der polizeilichen Tagebuchnummern oder staatsanwaltschaftlichen Aktenzeichen geschehen. Im vorliegenden Fall hatte die verantwortliche Stelle hierzu keine Angaben gemacht. Zudem ist der Zweck sehr allgemein gefasst, hier müssten seitens der verantwortlichen Stelle konkretere Angaben gemacht werden, z. B. welche Straftaten hier im Besonderen abgewehrt werden sollen. Nur so ist die Geeignetheit der einzelnen Kameras zu beurteilen, um die Erforderlichkeit feststellen zu können. Eine Erforderlichkeit für das Betreiben der Videokameras ist nur dann zu bejahen, wenn diese für den konkret festgelegten Zweck geeignet sind und keine mildereren Mittel zur Erreichung des Zwecks bei gleicher Effektivität vorhanden sind. Im vorliegenden Fall bestanden bei der Kamera im Wartebereich und auf dem Parkplatz Bedenken hinsichtlich der Geeignetheit für den jeweiligen Zweck, denn es wird nicht ersichtlich, welche Straftaten dort tatsächlich abgewehrt werden sollen. Zudem bestehen Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen das berechnete Interesse am Betreiben der Videoüberwachung überwiegen. Insbesondere im Wartebereich halten sich Personen typischerweise länger auf oder kommunizieren miteinander. In einem solchen Bereich kann der einzelne Bürger erwarten, nicht überwacht zu werden. Darüber hinaus wurden auf dem Parkplatz eine Vielzahl von dort parkenden Pkw und damit Personen erfasst. Ferner sind die Bewohner und Besucher der Immobilienverwaltungsgesellschaft auf die Nutzung des Parkplatzes angewiesen und können der Videoüberwachung nicht ausweichen.

Hinsichtlich der Kamera, welche auf die Fahrradständer und einen Teil des Gartenbereichs ausgerichtet ist, handelt es sich um einen nicht-öffentlichen Bereich, welcher nur von den Bewohnern des Hauses betreten werden kann. Die Zulässigkeit der dort angebrachten Kamera richtet sich dann nach § 28 Abs. 1 Nr. 2 BDSG, wonach die Datenerhebung und -verarbeitung sowie Nutzung als Mittel zur Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Insofern gilt das bereits im Rahmen der Prüfung von § 6b BDSG Gesagte. Auch hier ergeben sich Bedenken hinsichtlich der Geeignetheit für den genannten Zweck. Durch die verantwortliche Stelle muss hier genau konkretisiert werden, welche

Straftaten in diesem Bereich verhindert oder aufgeklärt werden sollen. Die Vorkommnisse aus der Vergangenheit können hier als Grundlage herangezogen werden.

Die Kameras, welche lediglich die Hauswand und einen Meter des Gehweges erfassten, waren datenschutzrechtlich als unbedenklich einzustufen, da diese gem. § 6 Abs. 1 Nr. 2 BDSG im Rahmen der Wahrnehmung des Hausrechts als zulässig zu betrachten sind.

Der TLfDI teilte der verantwortlichen Stelle seine Rechtsauffassung betreffend der betriebenen Videoüberwachungsanlage mit. Das Verwaltungsverfahren ist noch nicht beendet, sodass voraussichtlich in dem nächsten Tätigkeitsbericht über den Abschluss des Verfahrens berichtet werden wird.

Jede Entscheidung über eine Videoüberwachungsanlage ist eine Einzelfallentscheidung. Die einzelnen Kameras sind immer anhand des konkret festgelegten Zwecks zu beurteilen. Insbesondere die Erforderlichkeit der einzelnen Kamera kann nur so geprüft werden. Im vorliegenden Fall konnte noch keine abschließende Entscheidung getroffen werden, da weder ein berechtigtes Interesse am Betreiben der Kameras nachgewiesen wurde, noch konnte die Geeignetheit der betreffenden Kameras aufgrund des unkonkreten Zwecks abschließend bejaht werden. Die verantwortlichen Stellen sollten sich über diese Bereiche der Videoüberwachung genaue Gedanken machen und diese Festlegungen auch schriftlich zur Dokumentation festhalten. Die durch die Datenschutzaufsichtsbehörden erarbeitete „Orientierungshilfe Videoüberwachung für nicht-öffentliche Stellen“ wird auf der Website des TLfDI (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf) als Information und Hinweis bereitgestellt. Die hier genannten Schwerpunkte werden dort ausführlich dargestellt.



6.5 Video versus Vandalismus – Videogaga?

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass in direkter Nachbarschaft des Beschwerdeführers um 360° schwenkbare Kameras installiert worden seien, die beim Betreten und Verlassen des überwachten Bereiches Personen aufzeichneten. Diejenigen, die diesen Ort passierten – vor allem Mieter – seien von der Überwachung betroffen. Auch Fahrzeuge, die die öffentliche Straße in diesem Bereich nutzen, seien im Fokus der Aufnahmen.

Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdegegnerin gewandt und um die Beantwortung eines Fragenkataloges gebeten.

Zunächst berichtete die Beschwerdegegnerin in ihrer Antwort vom Anlass, der zur Objektüberwachung geführt habe. Seit etwa zwei Jahren hätten sich auf dem Objekt Sachbeschädigungsdelikte gehäuft und es sei dort vermehrt zu Verstößen gegen das Betäubungsmittelgesetz gekommen. Im Einzelnen seien gesteigert Fassadenteile beschmiert, Schaufenster der ansässigen Gewerbetreibenden verunstaltet und wiederholt Mülltonnen in Brand gesetzt worden. Einige der schwer einsehbaren Nischen auf dem Areal, wie z. B. die Garageneinfahrten und die Treppenaufgänge, seien von Unbekannten immer wieder für ihren Drogenkonsum genutzt worden. Insgesamt habe sich im Jahre 2014 eine Situation auf dem Areal dargestellt, die ein Verwahrlosen des Objektes ernsthaft befürchten ließ und zur zunehmenden Unsicherheit der Bewohner geführt habe. Um dem entgegenzuwirken, wäre das Ergreifen geeigneter Maßnahmen erforderlich gewesen. Zu diesem Zwecke sei ein Kamerasystem installiert worden, welches spürbar zu einem Rückgang an Straftaten geführt habe.

Den vom TLfDI zur Beantwortung gestellten Fragenkatalog indes konnte die Beschwerdegegnerin nur unzureichend beantworten, sodass der TLfDI in großem Maße Nachbesserungsbedarf sah, den er im Nachfolgenden präziserte.

Zu den einzelnen Kameras hatte sie, wie dargelegt, lediglich angegeben, dass sich auf dem Objektareal Sachbeschädigungsdelikte und Verstöße gegen das Betäubungsmittelgesetz gehäuft hätten.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung unter anderem zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen wird. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.

Der TLfDI bat in diesem Zusammenhang die Beschwerdegegnerin um Übermittlung von Nachweisen zu den von ihr erwähnten Vorfällen. Dies können beispielsweise Aktenzeichen von Anzeigen bei der Polizei oder auch bezahlte Rechnungen von Reparaturen sein.

§ 6b Abs. 1 Nr. 3 BDSG sieht vor, dass die mit der Kameraüberwachung verfolgten Zwecke konkret festgelegt werden. Das bedeutet, dass es für jede Kamera einer Festlegung bedarf, für welchen Zweck sie betrieben wird. Der TLfDI bat die Beschwerdegegnerin insoweit um Vorlage schriftlicher Festlegungen zu jeder Kamera mit Ausführungen dazu, warum die Kamera mit ihrem jeweiligen Aufnahmebereich für den verfolgten Zweck erforderlich ist.

In ihrer Rückantwort äußerte die Beschwerdegegnerin zunächst, dass mittlerweile – auf Hinweis des TLfDI – Hinweisschilder angebracht und die Speicherung auf 48 Stunden beschränkt worden seien.

Es hätte in der Vergangenheit, wie bereits dargelegt, zahlreiche Fälle von Graffiti-Schmierereien vor allem im Bereich der Gewerbeeinheiten gegeben. Zudem seien die Glasscheiben des Objekts der Beschwerdeführerin in diversen Fällen beschädigt worden, was stets zu teils kostenaufwendigen Reparaturen geführt habe. Diese Schäden seien jeweils, soweit bekannt, der Versicherung gemeldet worden.

Aktuell würden weitere Informationen hierzu zusammengetragen und dann an den TLfDI umgehend weitergeleitet werden.

Jede einzelne Kamera diene dem Zweck, Vandalismus-Schäden zu verhindern.

Eine Weiterbearbeitung der Akte wurde obsolet, als dem TLfDI mitgeteilt wurde, dass das streitgegenständliche Objekt veräußert worden war. Im Zuge dieser Veräußerung wurden die streitgegenständlichen Kameras entfernt.

Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen wird. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.

6.6 Pizza mit Draufsicht – Videogaga 1

Im Rahmen der Prüfung einer Sondernutzungserlaubnis für einen Biergarten wurde durch die zuständige Dienststelle einer Stadtverwaltung festgestellt, dass zwei kameraähnliche Gegenstände beidseitig am Bogen des Eingangsportals montiert waren. Die Kameras waren jeweils auf die links und rechts des Einganges befindlichen Stühle und Tische ausgerichtet. Ergänzend wurde noch mitgeteilt, dass durch die Erteilung einer Sondernutzungserlaubnis die Fläche nicht entwidmet worden war, sondern weiterhin der Öffentlichkeit zur Verfügung stand. Die Stadtverwaltung übergab den Fall zuständigkeitshalber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Der TLfDI verschaffte sich bei einer ersten Vor-Ort-Kontrolle einen Überblick. Zwei Kameras waren jeweils im Torbogen angebracht und auf einen großen öffentlichen Platz gerichtet. Es wird auch auf einem Display der Aufzeichnungsbereich gezeigt. Dabei konnte man erkennen, dass weite Teile des Gastraums sowie des Arbeitsbereiches (Küche) durch Kameras überwacht wurden. Insgesamt waren fünf Kameras im Einsatz.

Im Rahmen eines Auskunftsverlangens nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) stellte der TLfDI im Nachgang zu der Vor-Ort-Kontrolle verschiedene Fragen zur durch den Geschäftsführer der Restaurant GmbH betriebenen Videoüberwachungsanlage. Folgende rechtliche Beurteilung erging an den Betreiber: Die von der Restaurant GmbH betriebene Videoüberwachungsanlage ist derzeit insgesamt nicht mit dem BDSG vereinbar und wird damit rechtswidrig betrieben. Der Umgang mit personenbezogenen Daten steht unter einem sogenannten Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn das BDSG oder eine andere Rechtsvor-

schrift dies erlaubt, anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG.

Durch eine Videoüberwachungsanlage werden personenbezogene Daten erhoben und meist auch verarbeitet.

Eine Einwilligung scheidet in Fällen von Videoüberwachung regelmäßig aus, da sie grundsätzlich schriftlich und vor Datenerhebung bzw. -verarbeitung einzuholen ist. Soweit von der hier gegenständlichen Videoüberwachung auch Mitarbeiter betroffen waren, schied eine Einwilligung ebenfalls aus. Eine solche war ohnehin nur unter äußerst engen Voraussetzungen möglich, da hier in der Regel die für die Einwilligung notwendige Freiwilligkeit fehlte. Eine solche Freiwilligkeit kann nur dann gegeben sein, wenn dem Arbeitnehmer echte Alternativen zu einer Einwilligung aufgezeigt werden und dieser auch ohne eine solche seinen Arbeitspflichten nachkommen kann. Hier musste der videoüberwachte Bereich zwingend von den einzelnen Mitarbeitern betreten werden, weswegen es von vornherein an der verlangten Freiwilligkeit mangelte, da keine Alternativen zur Verfügung standen.

Hinsichtlich der fünf betriebenen Videokameras war keine gesetzliche Grundlage für den Datenumgang ersichtlich. Als Erlaubnisnorm kam ausschließlich § 6b BDSG in Betracht, da es sich sowohl beim Gastraum eines Restaurants, als auch bei der videoüberwachten Fläche vor dem Restaurant um einen öffentlich zugänglichen Raum handelte und diese spezielle und abschließende Regelung daher den übrigen Regelungen vorging. Zu prüfen war, ob die Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich war und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Betreiber hatte angegeben, dass die Beobachtung und Aufzeichnung zum Eigenschutz gegen Vandalismus und Diebstahl erfolgte, wobei er sodann detailliert ausführte, dass es für Ermittlungen in diesen Bereichen notwendig ist, entsprechende verwertbare Beweise zu schaffen. Dem konnte entnommen werden, dass der von ihm verfolgte Zweck der Videoüberwachung in der Verfolgung zivil- und strafrechtlicher Interessen lag. Diese sind ausschließlich im Rahmen der Voraussetzungen des § 6b Abs. 1 Nr. 3 BDSG zulässig, also zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.

Zwei der Kameras beobachteten weite Teile des öffentlichen Platzes der Innenstadt. Die Beobachtung dieser Bereiche war für die ange-

gebenen Zwecke nicht erforderlich. Außerdem gab es Anhaltspunkte, dass schutzwürdige Interessen Betroffener überwogen. Es handelte es sich um einen Platz, der tagsüber von einer unbestimmbaren Anzahl an Personen frequentiert wurde. Das Interesse dieser Personen, nicht in den Aufzeichnungsbereich der Kameras zu gelangen, überwog, weil sie unter Berücksichtigung des Zwecks der Videoüberwachung zu ihr in keiner Weise Anlass gegeben haben.

Auch im Fall der Kamera im Eingangsbereich waren deutliche Anhaltspunkte vorhanden, dass schutzwürdige Interessen Betroffener überwogen. Aufgezeichnet wurde nicht nur der Eingang des Restaurants, sondern ebenfalls eine Vielzahl an Sitz- und Stehgelegenheiten im Biergarten. Dieser Bereich diente zur Entspannung und Erholung sowie sonstigen Freizeitgestaltung. Das schutzwürdige Interesse der Gäste an einer unbeobachteten Freizeitgestaltung überwog aber das Interesse an einer dauerhaften Beobachtung der Gäste in den Sitzbereichen.

Hinsichtlich der Kamera, die den Zugang zur Toilette des Lokals und einen Zugang zum Notausgang beobachtete, war nicht ersichtlich, inwieweit durch diese Beobachtung dem Schutz vor einer Verletzung seines Eigentums durch Diebstahl und Vandalismus gedient werden sollte. Hier fehlte es an der Erforderlichkeit für die festgelegten Zwecke.

Letztlich verblieb die Kamera, die die Kochzeile beobachtete. Betroffene der Videoüberwachung waren ausschließlich die Arbeitnehmer. Im Ergebnis handelte es sich um eine Arbeitnehmerüberwachung. Diese ist nur unter der Maßgabe des § 32 Abs. 1 Satz 1 BDSG zulässig. Die Voraussetzungen der nach § 32 Abs. 1 Satz 1 BDSG zulässigen Arbeitnehmerüberwachung waren ebenfalls nicht erfüllt. Eine rein präventive Videoüberwachung ohne konkrete Anhaltspunkte für ein strafbares Verhalten von Mitarbeitern genügt den Anforderungen von § 32 Abs. 1 Satz 1 BDSG nicht (Seifert in Simitis, § 32 Rn. 80).

Nachdem der Betreiber die Videokameras am Eingang abmontiert, die Kameras im Gebäude mit Farbe unbrauchbar gemacht (Linse überstrichen) sowie den Bildschirm entfernt hatte, war das Verfahren beim TLfDI abgeschlossen. Dies wurde auch der zuständigen Stadtverwaltung mitgeteilt.

Der Umgang mit personenbezogenen Daten steht unter einem sogenannten Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Er-

hebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt, anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Das schutzwürdige Interesse der Gäste an einer unbeobachteten Freizeitgestaltung überwiegt grundsätzlich das Interesse an einer dauerhaften Beobachtung der Gäste in den Sitzbereichen einer Gaststätte.

6.7 Big Brother auf dem Marktplatz – Videogaga 2

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wegen einer Videoüberwachung an einem alten Einkaufsmarkt, die laut dessen Angaben auf den Marktplatz in einer thüringischen Stadt gerichtet war. Er fühlte sich beobachtet und bat um das Einschreiten des TLfDI. Da der TLfDI nach § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) sachlich zuständige Behörde zur Kontrolle der Ausführungen des BDSG ist, ging er dieser Anzeige im Rahmen seiner aufsichtsbehördlichen Tätigkeit nach.

Zunächst wurde beim zuständigen Gewerbeamt der Eigentümer des Gebäudes, an dem die Kamera installiert wurde, ermittelt. Dieser kam zunächst als verantwortliche Stelle gem. § 3 Abs. 7 BDSG in Betracht. Aufgrund dieser Angaben wandte sich der TLfDI mit einem Auskunftersuchen an den Eigentümer. Insbesondere wurde gefragt, ob überhaupt eine Videokamera installiert sei, da es regelmäßig vorkommt, dass sich Bürger über Videoüberwachungsanlagen beschweren und es sich nach – zeitraubenden – Ermittlungen herausstellt, dass es sich nur um einen Bewegungsmelder handelt, der das Licht einschalten soll. In diesem Fall bestätigte sich die Videoüberwachungsanlage.

Wenn eine Videokamera installiert ist, gilt es zu prüfen, welche gesetzlichen Regelungen Anwendung finden und ob diese eingehalten worden sind.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nämlich nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat in die Datenerhebung bzw. -verarbeitung eingewilligt.

Eine Einwilligung im Bereich der Videoüberwachung kommt nur in seltenen Ausnahmefällen in Betracht, da diese nach § 4 a Abs. 1 BDSG schriftlich und vor Erhebung der personenbezogenen Daten vorliegen muss. Diese strengen Voraussetzungen sind für die Betreiber der Videoüberwachung praktisch nicht umsetzbar, da der Betroffene zumeist vor Erteilung der Einwilligung bereits durch die Kameras aufgenommen wird und vor allem der Kreis der Betroffenen überhaupt nicht einzugrenzen ist. Als Erlaubnisnorm kommt hier § 6b BDSG in Betracht, welcher die Zulässigkeit der Beobachtung von öffentlich zugänglichen Räumen mit optisch-elektronischen Einrichtungen abschließend regelt. Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen.

Im vorliegenden Fall war nach Mitteilung durch den Bürger nicht von vornherein auszuschließen, dass öffentlicher Raum seitens des Eigentümers überwacht wurde. Dann ist für diesen Bereich die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen, § 6b BDSG. Der Gebäudeeigentümer teilte dem TLfDI zur Beantwortung des Auskunftersuchens mit, dass er eine Videoüberwachungsanlage installiert habe. Als Interesse gab der Eigentümer an, evtl. Einbrüchen, Diebstählen, Vandalismus und Brandstiftungen zu begegnen. Dies könnte zwar ein berechtigtes Interesse für die Installation einer Videokamera darstellen, jedoch muss von der verantwortlichen Stelle der Nachweis einer tatsächlichen Gefahrenlage verlangt werden. Diesen Umstand konnte der Eigentümer durchaus darstellen, denn es war zu einer Brandstiftung und einem Einbruch in den Räumlichkeiten einer dort befindlichen vermieteten Bar gekommen. Auch in der direkten Nachbarschaft war es zu Brandstiftungen und einem Raubüberfall gekommen.

Im Rahmen einer Videoüberwachung sind gemäß § 9 BDSG allerdings auch technisch-organisatorische Maßnahmen zu treffen, welche die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten. Entsprechende Maßnahmen sind in Anlage 1 zu § 9 BDSG aufgezählt. Ob in diesem Fall tatsächlich öffentlich zugänglicher Raum durch die Videoüberwachung erfasst wird, wird derzeit geprüft. Die Auswertung hierzu steht jedoch noch aus, sodass über

den Abschluss des Verwaltungsverfahrens voraussichtlich erst im kommenden Tätigkeitsbericht berichtet werden wird.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eine Einwilligung erteilt. Im Rahmen von Videoüberwachungen kommt für öffentlich zugängliche Räume nur § 6b BDSG als Erlaubnisnorm in Betracht. Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen. Auf private Eigentums- oder Besitzverhältnisse kommt es hingegen nicht an.

6.8 Videoüberwachung auf Firmengelände – Videogaga 3

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage einer Stadtverwaltung. Ein Bürger hatte sich dort über eine Firma beschwert, die eine Kamera an einem Beleuchtungsmast auf ihrem Grundstück installiert hatte und damit auch die am Firmengrundstück vorbeiführende Straße nebst Gehweg als öffentliche Verkehrsfläche überwache. Die Stadtverwaltung wollte sich nun erkundigen, ob die Kamera durch den TLfDI genehmigt worden sei.

Dem TLfDI lagen keine Informationen zu einer solchen Kamera vor, weswegen er sich mittels eines Auskunftersuchens an den Geschäftsführer der Firma wandte, um die Zulässigkeit der installierten Kamera zu prüfen. Dabei machte er darauf aufmerksam, dass das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig sei, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt. Öffentliche Verkehrsflächen sind öffentlich zugängliche Räume. Die Beobachtung und erst recht die Verarbeitung oder Nutzung der erhobenen Daten ist nur in engen Grenzen zulässig und zwar nur dann, wenn die Überwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen, § 6b Abs. 1 BDSG. Darüber hinaus sind der Umstand der Beobachtung und die verant-

wortliche Stelle durch geeignete Maßnahmen erkennbar zu machen, § 6b Abs. 2 BDSG.

Der Geschäftsführer des Unternehmens erklärte, dass der Aufnahmebereich dieser Kamera weder die Straße noch den entlangführenden Weg erfassen würde und wies dies mit Screenshots des Aufnahmebereichs nach. Außerdem seien Hinweisschilder angebracht worden. Er fügte einen Lageplan der Kameras bei und informierte den TLfDI, dass sich noch weitere Kameras auf dem Grundstück befinden. Die Kameraaufzeichnungen würden nach einer Woche überschrieben und damit gelöscht.

Einige Fragen blieben allerdings unbeantwortet. Zum Beispiel ist zur Beurteilung der Zulässigkeit die Angabe des Zwecks der Kameras notwendig. Darüber hinaus müsse der TLfDI erfahren, in welche Aufnahmebereiche die Kunden der Firma Zutritt haben und ob auch Bereiche überwacht werden in denen sich dauerhaft Arbeitnehmer aufhalten.

Im weiteren Verlauf teilte die Firma mit, der Zweck der Kameras sei die Wahrung des Hausrechts nach § 6b Abs. 1 BDSG. Die Kameras am Firmengebäude seien ausschließlich zur Sicherung des Gebäudes außerhalb der Geschäftszeiten, insbesondere gegen Einbruch, Diebstahl und Vandalismus, installiert. Schließlich habe es in dem Gewerbegebiet schon mehrfach und in unmittelbarer Nachbarschaft Einbrüche gegeben. Trotz Kameras habe man ergänzend einen Wachdienst beauftragt, der zudem zu bestimmten Zeiten das Objekt kontrolliere. Zur Betroffenheit von Mitarbeitern erläuterte der Geschäftsführer, dass ein dauerhafter Aufenthalt von Mitarbeitern im Kamerabereich ausgeschlossen sei, da die Kameras nur außerhalb der Geschäftszeiten aktiv seien und während der Geschäftszeiten keine Aufnahme stattfinde. Um sich ein genaueres Bild von den Kameras und deren Aufnahmebereichen zu machen, entschied der TLfDI, eine Kontrolle vor Ort durchzuführen.

Dabei wurde festgestellt, dass die Kamera an dem Lichtmast, auf die sich der Beschwerdeführer bezog, so eingestellt war, dass der öffentliche Weg nicht erfasst wurde und sie nur auf das Betriebsgrundstück gerichtet ist. Der von der Firma angegebene Zweck zur Wahrung des Hausrechts rechtfertigt dort eine Videoaufzeichnung, allerdings nur außerhalb der Geschäftszeiten. Ebenfalls nur außerhalb der Geschäftszeiten zulässig war eine auf eine Eingangstür gerichtete Kamera, in deren unmittelbarer Nähe ein Aschenbecher angebracht war,

weil dieser Bereich offenbar von den Mitarbeitern als Raucherbereich genutzt wurde.

Bei einer weiteren Kamera im Empfangsbereich innerhalb des Gebäudes war der Arbeitsplatz der Sekretärin ausgepixelt. Erfasst wurden jedoch die gläserne Haupteingangstür von innen und der Wartebereich für Besucher. Zur Zeit der Kontrolle war bei der Kamera die ständige Aufzeichnung aktiviert. Der TLfDI sah die Kameraüberwachung dann als entbehrlich an, wenn der Empfang besetzt ist. Ist der Platz nicht besetzt, kann eine Videoüberwachung erforderlich sein, da dann der freie Zugang zu mehreren Büros möglich ist.

Die Firmenleitung erwog darüber hinaus, eine weitere Kamera im Lagergebäude zu installieren. Diese würde dann Mitarbeiter und Lieferanten erfassen, um Diebstähle oder Verwechslungen der dort gelagerten Ware bzw. eine irrtümliche Mitnahme aufklären zu können. Die Mitarbeiter seien damit einverstanden. Hierzu wurde dem Geschäftsführer erläutert, dass die Einwilligung der Mitarbeiter die beabsichtigte Videoüberwachung mangels Freiwilligkeit nicht rechtfertigen kann. Auch für diese Videoüberwachung wurde keine Rechtsgrundlage gesehen, da es sich um einen Fall der Mitarbeiterüberwachung handelt, die Voraussetzung des § 32 BDSG jedoch nicht erfüllt ist. Auch aus § 28 BDSG kann eine Zulässigkeit der Videoüberwachung nicht angenommen werden, da davon auszugehen ist, dass schutzwürdige Interessen der Mitarbeiter überwiegen.

Nach § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sichtung des Materials notwendig ist, sollte innerhalb von zwei Tagen geklärt werden können. Die Firmenleitung sah jedoch eine längere Speicherung der Daten als notwendig an, da der Firmensitz an Wochenenden und über Feiertage länger als 48 Stunden unbesetzt sein kann. Der TLfDI hielt deswegen eine Speicherdauer von drei Tagen für zulässig.

Zu den Piktogrammen, welche auf die Videoüberwachung hinweisen, monierte der TLfDI den fehlenden Hinweis auf die verantwortliche Stelle. Die Firma versicherte, ein Hinweisschild in Auftrag zu geben, dass allen rechtlichen Vorschriften entspricht.

Erst wenn alle vom TLfDI verlangten Änderungen erfolgt sind und keine datenschutzrechtlichen Mängel mehr vorliegen, kann der Fall

abgeschlossen werden. Bis Redaktionsschluss war dies noch nicht der Fall.

Ein Grundstück gilt datenschutzrechtlich als öffentlich zugänglicher Raum, wenn es nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden darf. Anwendung findet dann der § 6b BDSG. Eine Videoüberwachung wäre zulässig, wenn sie zum Zweck der Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gemäß § 6b Abs. 2 BDSG ist der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen.

6.9 Tanken mit Stummfilm – Videogaga 4

Wie dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner Kontrolltätigkeit bekannt wurde, war in einer Thüringer Tankstelle eine Videoanlage installiert. Der Beschwerdeführer befürchtete aufgrund von Angaben der Mitarbeiter, dass an der Tankstelle eine Videoüberwachung mit Tonaufzeichnung stattfindet, da die Mitarbeiter angaben, dass der Stationsleiter über Gespräche in Kenntnis sei, an denen er nicht teilgenommen habe. Er teilte weiterhin mit, dass er auch mit dem Kontaktbereichsbeamten der Gemeinde bezüglich dieses Sachverhaltes Kontakt aufnehmen werde.

Der TLfDI wandte sich mit einem Auskunftersuchen nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) an den Inhaber, um den Sachverhalt aufzuklären. Der TLfDI legte dem Anschieben die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ bei, in welcher die Aufsichtsbehörden der Länder die Anforderungen an eine datenschutzgerechte Videoüberwachung darlegen. Die Orientierungshilfe ist unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_nicht-ffentliche-stellen.pdf auf der Homepage des TLfDI veröffentlicht.



https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_nicht-ffentliche-stellen.pdf auf der Homepage des TLfDI veröffentlicht.

Der Tankstellenbetreiber teilte mit, dass in der besagten Tankstelle keine Videoüberwachung stattfinde, da die Videoanlage wegen eines technischen Defektes außer Betrieb war, sie aber nach Behebung wieder in Be-

trieb genommen werden sollte.

Der TLfDI informierte den Betreiber darüber, dass vor dem Beginn einer neuerlichen Videoüberwachung seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen ist. Da es sich um ein Verfahren der automatisierten Datenverarbeitung handelte, musste durch den Betreiber entweder eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten nach § 4d Abs. 5 BDSG durchgeführt werden bzw. falls ein solcher nicht bestellt war, musste dem TLfDI eine Meldung nach § 4d Abs. 1 BDSG gemacht werden. Der Inhalt der Meldung ergibt sich dabei aus § 4e Satz 1 BDSG. Der Betreiber wurde gebeten, dem TLfDI vor der Inbetriebnahme der Videoüberwachung entweder die Vorabkontrolle des betrieblichen Datenschutzbeauftragten bzw. die Meldung nach § 4d Abs. 1 BDSG zuzusenden. Ihm wurden das Hauptblatt zum Meldeformular sowie das Anlagenformular zugesandt, das grundsätzlich für jedes Verfahren automatisierter Verarbeitung auszufüllen ist.

Der Betreiber kam den oben genannten Aufforderungen nach, indem sein betrieblicher Datenschutzbeauftragter eine Vorabkontrolle nach § 4d Abs. 5 BDSG durchführte und alle Kameras so ausrichtete, dass Mitarbeiter nicht im Bereich der Kasse aufgenommen wurden. Teils wurden die Bilder entsprechend verpixelt, teilweise die Kameras neu ausgerichtet. Die Videoanlage wurde erst wieder in Betrieb genommen, nachdem eine positive Bewertung der rechtlichen Zulässigkeit vom TLfDI vorlag.

Die Überwachung von öffentlich zugänglichen Flächen und Arbeitsplätzen, wie in diesem Fall in einer Tankstelle, ist **nur** zur Wahrnehmung des Hausrechts oder beim Vorliegen berechtigter Interessen für konkret festgelegte Zwecke (etwa konkreter Diebstahlsverdacht) zulässig. Es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Tonaufnahmen sind nicht zulässig. Zur rechtskonformen Videoüberwachung gehört nicht nur die Berücksichtigung schutzwürdiger Interessen der Kunden, sondern auch derjenigen der Mitarbeiter im Rahmen des Arbeitnehmerdatenschutzes.

6.10 Smart-Home-Präsentation: inklusive Videoüberwachung

Im Juni 2016 informierte ein anonymer Anrufer den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in den Geschäftsräumen eines Sparberaters für Telekommunikation eine Videokamera installiert sei, die von der Eingangstür in den Innenraum gerichtet ist. Dabei handele es sich vermutlich um eine „Smart-Home-Lösung“, die den Zugriff per App zulasse. Der Anlageberater habe nur wenige Mitarbeiter, die jedoch durch die Kamera erfasst würden.

Aufgrund des Anrufs und zur Prüfung der rechtlichen Zulässigkeit wandte sich der TLfDI schriftlich an den Sparberater und bat um Auskunft darüber, ob in seinen Geschäftsräumen eine Videokamera im Einsatz ist und inwiefern diese zur Überwachung genutzt wird.

Der Sparberater beantwortete die Fragen des TLfDI zur Kameraüberwachung ausführlich und legte dar, dass es sich nicht um eine Kamerainstallation zur Überwachung von Passanten und Kunden handelte, sondern um eine Smart-Home-Präsentationswand eines deutschen Telekommunikationsunternehmens, die für Vorführungen mit den Kunden genutzt wird. Anhand von Skizzen zur Anordnung der technischen Geräte wurden die Ausführungen untermauert. Nach Darlegung des Sparberaters war diese Präsentationswand ausgerüstet mit verschiedenen sicherheitstechnischen Komponenten, unter anderem einem Rauchmelder, einem Heizthermostat, einem sirenengekoppelten Fensterkontakt und einer Videokamera. Die Kunden können diese technischen Komponenten nach ihrer funktionellen Vorführung erwerben. Darüber hinaus wird diese Sicherheitstechnik außerhalb der Öffnungszeiten als Schutz vor Einbrüchen genutzt und in diesem Sinne zu bestimmten Zeiten eingeschaltet. Im Alarmfall erfolge dann eine digitale Videoaufzeichnung. Nur in diesem Falle werden die Daten gespeichert von Personen, die sich unbefugt Zutritt zu den Räumen verschafft haben.

Aufgrund der Darlegungen des Sparberaters sah der TLfDI die Angelegenheit als erledigt an und keine Notwendigkeit, weitere Maßnahmen zu ergreifen.

Wenn ein Berater für Energieeinsparung und/oder Sicherheitstechnik in seinen Geschäftsräumen entsprechende Technik zu Demonstrationszwecken einsetzt (Videoüberwachung, Bild- und Tonaufnahmetechnik etc.), und eine Videoaufzeichnung nur im Alarmfall stattfin-

det, wenn die Technik gleichzeitig als Schutz vor Einbrüchen eingesetzt wird, liegt kein Verstoß gegen Datenschutzrecht vor.

6.11 Video für Baufortschritt – kein Fortschritt – Videogaga 5

Im Juni 2016 wandte sich der Vorsitzende eines Sportvereins an den TLfDI und bat um die Genehmigung zur Aufstellung einer Videokamera. Die Gemeinde beabsichtigte, den Sportplatz umfassend zu sanieren und der Verein wollte dies mit einer Baustellenkamera dokumentieren. Der Vereinsvorsitzende übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) alle Informationen über den Standort der Kamera und deren Aufnahmebereich. Der Vereinsvorsitzende teilte mit, dass die Kamera so ausgerichtet werden könne, dass nur die Baustelle selbst in den Beobachtungsbereich der Kamera fällt. Es sollten keine durchgehenden Videoaufnahmen erstellt werden, sondern beispielsweise nur stündlich ein Foto. Die Fotos sollten dann hintereinander geschnitten werden, um so im Zeitraffer den Baufortschritt verfolgen zu können. Der TLfDI beantwortete die Anfrage des Vereinsvorsitzenden folgendermaßen:

Der TLfDI ist als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich keine Genehmigungsbehörde für den Einsatz von Videoüberwachung. Eine derartige Maßnahme kann durchgeführt werden, sofern eine Rechtsvorschrift sie erlaubt oder der jeweils Betroffene zugestimmt hat, das sogenannte Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG).

Da aufgrund der gestellten Anfrage nicht eindeutig klar war, ob es sich bei dem Bereich, der aufgenommen werden sollte um einen öffentlich zugänglichen Bereich handelte, erläuterte der TLfDI die Rechtslage allgemein:

Die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Geräten, d. h. Videoüberwachung, ist in § 6b BDSG geregelt. Danach ist die Videoüberwachung nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Das heißt, wenn öffentlich zugängliche Räume von der geplanten Videoüberwachung betroffen sind, ist diese Maßnahme nur zu Dokumentationszwecken der Baufortschritte nicht zulässig, da hier schutzwürdige Interessen der Betroffenen entgegenstehen. Es

werden nämlich ohne Anlass alle Personen gefilmt, die sich in den Aufnahmebereich der Kamera begeben.

Im Sinne der Verkehrssicherungspflicht müssen Baustellen so abgesperrt sein, dass sie nicht von anderen Personen als den Baustellenarbeitern betreten werden können. Somit ging der TLfDI im vorliegenden Fall davon aus, dass der Baubereich kein öffentlich zugänglicher Bereich ist. Sofern kein öffentlich zugänglicher Raum beobachtet wird, beurteilt sich die Zulässigkeit der Videoüberwachung nach § 28 BDSG. Gemäß § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung für die Erfüllung von eigenen Geschäftszwecken zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Als Betroffene von der Videoüberwachung sind hier im Wesentlichen die Baustellenmitarbeiter, Architekten usw. anzusehen. Aus datenschutzrechtlicher Sicht ist die geplante Videodokumentation nur dann unbedenklich, wenn folgende Regeln eingehalten werden:

- die Ausrichtung der Kamera und die qualitative Auflösung der Bilder dürfen keine Identifizierung der arbeitenden Personen zulassen,
- die Betroffenen müssen im Vorfeld über die Maßnahme informiert werden und
- die Betroffenen müssen über die Beteiligungsrechte ihrer Interessenvertretungen informiert werden.

Aus datenschutzrechtlicher Sicht empfahl der TLfDI, nur Übersichtsaufnahmen ohne Personenbezug von der Baustelle anzufertigen, da dann die schutzwürdigen Interessen der Betroffenen nicht tangiert werden.

Der TLfDI bat den Vereinsvorsitzenden darum, ihm Testaufnahmen der Kamera zur Verfügung zu stellen. Hierbei wurde deutlich, dass aufgrund der qualitativ guten Aufnahme jeder Passant und jeder Bauarbeiter, der sich in diesem Bereich aufhielt, erkennbar war. Der TLfDI wies den Vereinsvorsitzenden darauf hin, dass für solche personenbezogenen Aufnahmen die Rechtsgrundlage fehle. Da sich die Bauarbeiter in einem Beschäftigungsverhältnis zum Auftragnehmer befinden, können sie auch keine freiwillige Einwilligung zu den Aufnahmen abgeben, da sie aufgrund des bestehenden Abhängigkeitsverhältnisses nicht frei entscheiden können. Weiterhin war in

den Erfassungsbereich der Kamera ein Weg einbezogen, der von Spaziergängern und als Zugang zum Sportplatz genutzt wurde. Für die Videoüberwachung dieses öffentlich zugänglichen Bereichs fehlte ebenfalls die Rechtsgrundlage. Eine Möglichkeit, die Kamera höher anzubringen (beispielsweise an Flutlichtmasten), um den Aufnahmebereich einzuschränken, bestand nicht.

Daher riet der TLfDI dem Vereinsvorsitzenden datenschutzrechtlich zu folgender Verfahrensweise: Die Kamera sollte lediglich zu einem bestimmten Zeitpunkt nach Ende der Bautätigkeit (ab 18:00 Uhr) für eine Momentaufnahme in Betrieb gesetzt werden, um den Fortschritt der Bautätigkeit zu dokumentieren. Der Vereinsvorsitzende sollte auf dem gesamten Sportplatz Hinweisschilder anbringen, damit jeder rechtzeitig den Aufnahmebereich der Kamera verlassen kann, der nicht auf der Aufnahme gespeichert werden will. Sollten sich auf den Momentaufnahmen nach Durchsicht dennoch Personen befinden, sollten diese nachträglich, beispielsweise mittels Pixeln, unkenntlich gemacht werden. Der Vereinsvorsitzende setzte die Anforderungen des TLfDI um.

Als nicht-öffentliche Stellen unterliegen Vereine den Regelungen des BDSG. Die Installation einer Videokamera zu Dokumentationszwecken einer den Verein betreffenden Baumaßnahme ist zulässig, wenn nur Übersichtsaufnahmen erstellt werden und das Recht des Einzelnen auf informationelle Selbstbestimmung nicht berührt wird. In diesem Sinne sollte die Videokamera erst am Abend, nach Ende der Bautätigkeit, für Momentaufnahmen in Betrieb genommen werden. Des Weiteren sind rund um den Kamerabereich Hinweisschilder zu Aufnahmezeit und Aufnahmebereich der Kamera anzubringen.

6.12 Videoüberwachung der Insolvenzmasse

Im Berichtszeitraum informierte eine Polizeiinspektion (PI) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in einem Wohngebiet der Stadt an einem Wohnblock und auf dem zugehörigen Grundstück mehrere Kameras installiert seien. Die PI belegte den Sachverhalt zusätzlich mit entsprechenden Fotoaufnahmen.

Der TLfDI wandte sich zunächst an das Grundbuchamt und bat um Amtshilfe zur Ermittlung des Eigentümers nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG). Das Grundbuchamt teilte dem TLfDI

Namen und Anschrift des eingetragenen Hauseigentümers mit. Das Grundstück gehörte einem Privatunternehmen, das sich in Insolvenz befand und für das ein Insolvenzverwalter bestellt war.

Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Nach § 4 Abs. 1 BDSG bedarf die Erhebung von Videoaufnahmen einer gesetzlichen Ermächtigung oder der Einwilligung des Betroffenen. Daher bat der TLfDI den Insolvenzverwalter gemäß § 38 Abs. 3 Satz 1 BDSG um eine detaillierte Auskunft zur installierten Videoanlage. Daraufhin teilte der Rechtsanwalt des Insolvenzverwalters dem TLfDI mit, dass sein Mandant inzwischen sämtliche Kameras am betreffenden Gebäude und auf dem Grundstück demonstrieren ließ. Ausweislich einer dem Schreiben beigefügten Hausmeisterrechnung war die Demontage Ende Dezember 2016 erfolgt.

Daraufhin teilte der TLfDI dem Rechtsanwalt des Insolvenzverwalters mit, dass die Angelegenheit somit datenschutzrechtlich erledigt sei und behielt sich eine Vor-Ort-Kontrolle vor. Weiterhin informierte der TLfDI die PI darüber, dass die Kameras demontiert wurden.

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“ (§ 4 Abs. 1 BDSG). Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Er kontrolliert nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Einhaltung entsprechender datenschutzrechtlicher Bestimmungen.

6.13 Der (Tür)Spion, der die Nachbarn nicht liebte; Videogaga 6

Die Beschwerdeführer wandten sich gegen die Installation einer digitalen Türspion-Kamera, mit der ein Mitmieter sie und andere in dem von ihnen bewohnten Mehrfamilienhaus beobachten würde.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat die Betreiber der Anlage um Auskünfte, welche Bereiche zu welchen Zwecken und seit wann video-

überwacht, auf welche Art und Weise die erhobenen Daten gespeichert und wie lange die Überwachungsdaten aufbewahrt werden. Daraufhin teilten die Beschwerdegegner mit, dass sich an ihrer Wohnungstür ein digitaler Türspion befinde, durch welchen die Personen vor ihrer Wohnungstür beobachtet werden könnten. Eine Speicherung der Daten erfolge nicht.

Bei einer Videoüberwachung, die auf einen allgemein zugänglichen Hausflur gerichtet ist, handelt es sich stets um einen Umgang mit personenbezogenen Daten. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG.

Im Falle einer Videoüberwachung scheidet eine zu einer Zulässigkeit der Anlage führende Einwilligung der Betroffenen in aller Regel aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Daher bedarf es einer Rechtsvorschrift, die diese Videoüberwachung erlaubt.

Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage von öffentlich zugänglichen Bereichen ist regelmäßig § 6b BDSG. Nach § 6b Absatz 1 BDSG ist die Videoüberwachung eine Beobachtung mit optisch-elektronischen Einrichtungen. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Hierunter fällt auch der digitale Türspion. Die Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor, so auch beim digitalen Türspion, erfolgt, als auch die Videoaufzeichnung, bei der Aufnahmen gespeichert werden.

Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum (z. B. Hauseingang oder öffentlicher Verkehrsraum) beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb und außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. Grundstückseigentümer, Vermieter etc.) von jedermann genutzt oder betreten werden dürfen. Bei einer Videoüberwachung im Innenbereich von Mehrfamilienhäusern handelt es sich in der Regel nicht um öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b BDSG richtet. In diesen Fällen greift § 28 Abs. 1 Nr. 2 BDSG, wonach aber ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG.

Die Überwachung des Treppenhauses mit einem digitalen Türspion – unabhängig davon, dass lediglich eine Aufzeichnung und keine Speicherung von Aufnahmen erfolgt – stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Nachbarn dar. Im nicht-öffentlich zugänglichen Raum hat die Privatsphäre eine noch höhere Bedeutung als im öffentlich zugänglichen Raum, denn die anderen Mieter und Mieterinnen sind sich bewusst, dass sie sich in einem Bereich befinden, zu dem nur eine begrenzte Zahl von Personen Zutritt hat. Der Überwachungsdruck wird hier deshalb zumeist noch stärker wahrgenommen als im öffentlich zugänglichen Bereich.

Personenbezogene Daten – hier: Bilddaten – können zur Wahrnehmung berechtigter Interessen nur dann erhoben, gespeichert, verändert oder übermittelt werden, soweit dies erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss einer Videoüberwachung überwiegen. Die Zwecke, für die die Daten genutzt werden sollen, sind vor der Erhebung konkret festzulegen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.

Der Einbau einer Türkameraanlage zur Einlasskontrolle ist grundsätzlich datenschutzrechtlich unbedenklich, wenn er jeweils nur anlassbezogen durch das Klingeln an der Tür aktiviert wird, sich der Monitor anschaltet, wenn geklingelt wird, sie nur den unmittelbaren Eingangsbereich vor der Tür erfasst, in dem sich die klingelnde Person aufhält, sie nach kurzer Zeit automatisch wieder deaktiviert wird und keine Aufzeichnung der Bilder erfolgt. Außerdem muss sich an der Tür bzw. der Türklingel ein deutlich sichtbares Hinweisschild befinden, das auf die Kamera aufmerksam macht.

Als Begründung für die Überwachung führten die Beschwerdegegner im vorliegenden Fall aus, sie wollten so verhindern, dass sie weiterhin durch verletzendes Bemerkungen der Beschwerdeführer gemobbt würden. Hierbei handelt es sich zwar um ein berechtigtes Interesse, jedoch ist die Videoüberwachung mittels des digitalen Türspions nicht für ihren Zweck – Vorbeugung von Mobbing – geeignet.

Außerdem bestehen Anhaltspunkte, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen. Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mithilfe von Kameras beobachtet oder aufgezeichnet wird. Die Tatsache, beobachtet zu werden, bewirkt bei vielen Personen eine Änderung ihres Auftretens. Das eigene Verhalten wird überprüft. Zudem sieht sich der Einzelne einem permanenten Überwachungsdruck ausgesetzt, der eine Beeinträchtigung des Persönlichkeitsrechts darstellt (siehe auch: Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 [BVerfGE 65, 1] – Volkszählung). Nach dieser Entscheidung wird unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig.

Der TLfDI hat den Beschwerdegegnern daher mitgeteilt, dass die von ihnen betriebene Videoüberwachungsanlage in der jetzigen Form nicht mit dem BDSG vereinbar ist.

Auf den Hinweis des TLfDI haben die Beschwerdegegner die Türkamera wieder durch einen „normalen“ Türspion ersetzt.

Im Innenbereich von Mehrfamilienhäusern handelt es sich in der Regel nicht um öffentlich zugängliche Räume, sodass bei einer Videoüberwachung in diesen Fällen nicht § 6b BDSG, sondern § 28 Abs. 1 Nr. 2 BDSG anzuwenden ist, bei dem ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. Die Überwachung des Treppenhauses durch einen digitalen Türspion – unabhängig davon, dass lediglich eine Aufzeichnung, aber keine Speicherung von Aufnahmen erfolgt – stellt einen erheblichen Eingriff in das Persönlichkeitsrecht und Selbstbestimmungsrecht der Nachbarn dar, sodass ein solcher nur unter bestimmten Umständen als zulässig anzusehen ist.

Bei der Installation einer Türkameraanlage zur Einlasskontrolle bestehen dabei grundsätzlich keine datenschutzrechtlichen Bedenken, wenn sie jeweils nur anlassbezogen durch das Klingeln an der

Tür aktiviert wird, sich der Monitor anschaltet, wenn geklingelt wird, sie nur den unmittelbaren Eingangsbereich vor der Tür erfasst, in dem sich die klingelnde Person aufhält, sie nach kurzer Zeit automatisch wieder deaktiviert wird und keine Aufzeichnung der Bilder erfolgt. Außerdem muss an der Tür bzw. der Türklingel ein deutlich sichtbares Hinweisschild angebracht sein, das auf die Kamera aufmerksam macht.

6.14 Man kann den Pelz nicht waschen, ohne sich nass zu machen: Videogaga 7

Die Beschwerdeführer wandten sich zunächst mündlich und sodann schriftlich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wegen der Installation einer Kamera, die sie und andere permanent beobachte.

Ihr Grundstück sei Teil einer Reihenhaussiedlung. Der Beschwerdegegner habe offensichtlich und auffallend an seinem Gebäude eine Kamera in einem Fenster im ersten Stock angebracht. Diese Kamera sei nach mehrfacher Änderung der Befestigung am Fenster jetzt unmittelbar am Haus angebracht.

Eine derartige Kamera mit einem nicht verstellbaren Blickwinkel von ca. 100 bis 110 Grad dürfte ohne ihr Einverständnis nicht zulässig sein. Sie fühlten sich durch diese Beobachtung in ihrer Privatsphäre eingeschränkt und bedroht.

Wie den Beschwerdeführern bereits telefonisch mitgeteilt wurde, ist der TLfDI die zuständige Aufsichtsbehörde für den Datenschutz, § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG). Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

In dieser Funktion beabsichtigte der TLfDI, sich in dieser Angelegenheit an den Beschwerdegegner zu wenden, um die Zulässigkeit der Videoüberwachung zu prüfen.

Er bat die Beschwerdeführer in diesem Zusammenhang zunächst, ihm den Namen des Beschwerdegegners und damit mutmaßlichen Betreibers der Videokamera zukommen zu lassen.

Ohne Kenntnis des Namens des Beschwerdegegners kann der TLfDI diesen nur mit erheblichem Zeitaufwand oder gar überhaupt nicht nach § 38 Abs. 3 BDSG zur Auskunftserteilung auffordern.

Daneben hat der TLfDI die Beschwerdeführer auf die Möglichkeit hingewiesen, privatrechtlich gegen die vermeintliche Videoüberwachung vorzugehen. Sollten sie dies anstreben, habe dies keinen Einfluss auf das Tätigwerden des TLfDI. Eine Beratung dazu könne aber leider nicht erfolgen.

Darauf erwiderten die Beschwerdeführer, den Namen des Beschwerdegegners preiszugeben, sei nicht angezeigt, weil dies zwangsläufig zu einer Eskalation führe.

Mangels fehlender Zuarbeit einerseits und der Erkenntnis der Beschwerdeführer andererseits, dass die Einschaltung des TLfDI für das Nachbarschaftsverhältnis nicht förderlich sei, hat der TLfDI die Akte schließlich geschlossen.

Ohne Kenntnis der Adresse und des Namens des Beschwerdegegners kann der TLfDI diesen nur mit erheblichem Zeitaufwand oder überhaupt nicht nach § 38 Abs. 3 BDSG zur Auskunftserteilung auffordern, um dann gegebenenfalls Maßnahmen zu ergreifen.

6.15 Bei Klingeln Aufnahme: BDSG?

Im April 2016 informierte ein Bürger den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass im Klingeltableau am Gebäude eines Wohnhauses eine Kamera integriert sei und diese Kamera von einem privaten Grundstückseigentümer installiert wurde. Diese Kamera sei so angebracht, dass damit die gesamte Straße eingesehen und überwacht werden könne. Der Beschwerdeführer legte dar, dass er selbst diese Straße regelmäßig benutze und dabei sichergestellt wissen wolle, dass keine Privatperson diesen öffentlichen Verkehrsraum überwachen kann.

Der TLfDI prüfte den Sachverhalt und konnte jedoch keinen datenschutzrechtlichen Verstoß feststellen. Die im Klingeltableau integrierte Kamera wurde nur bei Betätigung der Klingel aktiviert und übertrug dabei ein Bild des Eingangsbereichs sowie von der klingelnden Person. Es war nicht möglich, mithilfe der Kamera den Eingangsbereich zu „überwachen“, d. h. der Wohnungseigentümer konnte ohne ein Klingelsignal nicht einfach „nachschaun“ ob sich jemand im Bereich der Klingel befand, da die Bildübertragung erst

durch das Klingeln ausgelöst wurde. Weiterhin wurde die Bildübertragung nach zehn Sekunden unterbrochen. Ein dauerhaftes Aufzeichnen bzw. eine Beobachtung mit der Klingelkamera war nicht möglich.

Datenschutzrechtlich sind solche Klingel-Videoanlagen in der Regel zulässig. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten nur dann erhoben, verarbeitet oder genutzt werden, wenn ein Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Einwilligungen scheiden bei Videoüberwachungen regelmäßig aus. Allerdings regelt der Gesetzgeber in § 6b BDSG die Beobachtung öffentlich zugänglicher Bereiche abschließend. Danach beurteilen sich auch solche Videokameras, die bei Betätigung der Klingel für kurze Zeit angehen, wenn dabei solche Bereiche erfasst werden, so wie es hier der Fall war.

Die Bildübertragung stellt dabei ein berechtigtes Interesse des Klingelbetreibers dar, was nach § 6b Abs. 1 Nr. 2 BDSG einen der zulässigen Anwendungsbereiche für Videoüberwachung darstellt. Auch gibt es keine Anhaltspunkte dafür, dass bei der Kürze der Beobachtung schutzwürdige Interessen Dritter überwiegen. Eine Speicherung erfolgt nicht.

Voraussetzung für diese Einschätzung ist, dass die Kamera nur aktiv wird, wenn geklingelt wird, und sich innerhalb weniger Sekunden wieder deaktiviert. Ebenfalls darf sie nicht aus der Wohnung heraus aktivierbar sein.

Eine in die Hausklingel integrierte Kamera, die nur durch Betätigung der Klingel ausgelöst wird und dann nur eine kurze, wenige Sekunden dauernde Videosequenz des Besuchers an den Wohnungs- bzw. Hauseigentümer überträgt, ist nach § 6b Abs. 1 BDSG in der Regel zulässig.

6.16 Fenster zum Hof

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass an einem Gebäude eine offensichtlich nicht datenschutzgerechte Videoüberwachungsanlage betrieben werde. Bei dieser Videoüberwachungsanlage handele es sich um insgesamt fünf Kameras, die auf den öffentlich

zugänglichen Bereich ausgerichtet seien. Davon befänden sich zwei Kameras an den Fenstern in der ersten Etage und drei Kameras an den Fenstern im Erdgeschoss.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei Videoaufnahmen handelt es sich um ein Erheben von personenbezogenen Daten, die nach § 4 Abs. 1 des BDSG einer gesetzlichen Ermächtigung bedürfen.

Der TLfDI hat sich daher mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an den Beschwerdegegner gewandt und bat um die Beantwortung eines Fragenkataloges, um den Sachverhalt zu ermitteln.

So wurde der Beschwerdegegner unter anderem befragt, ob er an dem o. g. Gebäude eine Videoüberwachungsanlage betreibe, welche Bereiche zu welchen Zwecken und seit wann videoüberwacht werden.

Der Beschwerdegegner hat in seiner Antwort eingeräumt, Attrappen wegen Verunreinigungen und Beschädigungen seines Eigentumes – unter anderem durch Tiere – einzusetzen. Seit Anbringen der Attrappen gäbe es keine neuen Schäden an seinem Eigentum.

Der TLfDI gab in seiner Erwiderung zu bedenken, dass davon gleichsam ein Überwachungsdruck ausgehe. Auch solche Einrichtungen müssten den im Bundesdatenschutzgesetz (BDSG) geregelten Anforderungen entsprechen, um eine rechtswidrige Verletzung von Grundrechten anderer Bürger zu vermeiden.

Insofern sollte auch bei Verwendung von Attrappen geprüft werden, ob die datenschutzrechtlichen Vorgaben eingehalten werden. In allen Bereichen, in denen sich danach der echte Kameraeinsatz verbietet, sollte somit auch der Einsatz von Kameraattrappen einer Prüfung unterzogen werden. Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Daher bedarf es auch hier einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn, es handelt sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Die Europäische Datenschutz-Richtlinie sieht für die Daten-

verarbeitung mittels Videoüberwachung eine Ausnahme vor, wenn die Verarbeitung von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (sog. household exemption). Diese Ausnahme ist nach Ansicht des EuGH allerdings eng auszulegen (Urt. v. 11. Dezember 2014, Az. C-212/13). Daher könne eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre gerichtet ist, nicht als eine „ausschließlich persönliche oder familiäre Tätigkeit“ angesehen werden. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen erfasst werden, die mit dem Videobetreiber nicht in enger familiärer Beziehung stehen. Spätestens an Grundstücksgrenzen endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel. Nach Sichtung der dem TLfDI vorliegenden Fotos und nach dem Vortrag des Beschwerdegegners sind die Kameraattrappen auch auf die angrenzende öffentliche Straße und den Fußweg ausgerichtet, sodass auch Passanten, Nachbarn oder andere Betroffene in den Erfassungsbereich der Kameraattrappen gelangen können, die in keiner persönlichen oder familiären Verbindung zum Kamerabetreiber stehen.

Kameras, die neben dem eigenen Grundstück/Hof auch den öffentlich zugänglichen Raum in der Umgebung, wie die angrenzende Straße und den Gehweg und die dort befindlichen Personen, mit erfassen, sind nach § 6b BDSG zu beurteilen. Danach ist eine Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Auch bevor eine Kameraattrappe installiert wird, sollte festgelegt werden, welches Ziel damit erreicht werden soll. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.

Im Schreiben des Beschwerdegegners sind, wie erörtert, Vorkommnisse genannt. Den genauen Zweck der Kameraattrappen hatte er bisher aber nicht angegeben. Nach derzeitiger Aktenlage diene die

vom Beschwerdegegner durchgeführte vermeintliche Videoüberwachung und die damit verbundene abschreckende Wirkung der Verhinderung künftiger Beschädigungen. Daher bat der TLfDI um eine detaillierte Aufstellung der Vorkommnisse und ggfls. entsprechende Nachweise.

Der Beschwerdegegner teilte indes mit, dass er aufgrund des oben genannten Schreibens des TLfDI die Kameraattrappen entfernen werde, was in der Folgezeit geschah.

Mit dieser Information sah der TLfDI das Verfahren als erledigt an.

Grundsätzlich sollten Attrappen nach den gleichen Maßstäben wie tatsächlich funktionsfähige Kameras zu beurteilen sein, da von ihnen ein ähnlicher Überwachungsdruck ausgeht. Auch solche Einrichtungen sollten den im Bundesdatenschutzgesetz (BDSG) geregelten Anforderungen entsprechen, um eine rechtswidrige Verletzung von Grundrechten anderer Bürger zu vermeiden.

6.17 Auskunftsverweigerungs(un)recht

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat Kenntnis davon erlangt, dass ein Beschwerdegegner an der Fassade seines Gebäudes vier Kameras angebracht habe. Neben dem Gebäudeeingang soll sich zudem ein Monitor befinden, auf welchem vier jeweils sich bewegende Kameramitschnitte zu sehen seien. Auf diesen Mitschnitten, die das Grundstück des Beschwerdegegners betreffen, sei wiederum zu sehen, dass nicht nur sein Privatgrundstück, sondern auch der öffentliche Verkehrsraum erkennbar wäre.

In mehreren Schreiben wandte sich der TLfDI vergeblich an den Beschwerdegegner mit der Aufforderung, sich – jeweils unter Fristsetzung - zum Sachverhalt zu äußern und insbesondere die dort gestellten Fragen zu beantworten. Trotz dieser Fristsetzungen hat sich der Beschwerdegegner zu dem Vorgang nicht geäußert.

Nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) hat die verantwortliche Stelle, vorliegend der Beschwerdegegner, dem TLfDI auf dessen Verlangen die für die Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Im Streitfalle betrifft dies vor allem die Frage, ob und bejahendenfalls in welchem Umfang der Beschwerdegegner eine Videoüberwachung betreibt. Nach § 38 Abs. 3 Satz 2 kann der Verpflichtete die Auskunft von

Fragen unter den dort genannten Voraussetzungen verweigern. Die möglichen Gründe einer Auskunftsverweigerung sind ebenfalls in der vom TLfDI gesetzten Frist diesem gegenüber zu erklären.

Der TLfDI hat dem Beschwerdegegner zu diesem Zweck einen Bescheid auf Auskunftserteilung zugestellt, um auf diesem Wege die begehrten Auskünfte zu erlangen. Daraufhin erteilte der Angeschriebene endlich Auskunft. Nach Auswertung der Informationen wurde festgestellt, dass öffentlich zugängliche Bereiche von der Videoüberwachung nicht betroffen waren. Das Verfahren konnte beendet werden.

Nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) hat die verantwortliche Stelle dem TLfDI auf dessen Verlangen die für die Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen, wenn nicht ausnahmsweise ein Auskunftsverweigerungsrecht besteht. Diese Auskünfte können auch durch Vollstreckung des Verwaltungsaktes erzwungen werden. Bestes Mittel ist hierfür regelmäßig das Zwangsgeld. Der TLfDI ist auch ermächtigt, in Fällen, in denen nicht, nicht richtig oder nicht rechtzeitig Auskunft erteilt wird, ein Bußgeldverfahren einzuleiten. Hiervon macht er regelmäßig Gebrauch.

6.18 Der abgeschottete Nachbar

Im Berichtszeitraum 2014/2015 hatte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber beschwert, dass in seiner Nachbarschaft eine Überwachungskamera am Carport angebracht worden sei. Der Beschwerdeführer mutmaßte, dass mit der Kamera der Eingangsbereich seines Hauses überwacht würde und ebenso der Verkehrsraum einer öffentlichen Straße. Er bat den TLfDI um eine datenschutzrechtliche Überprüfung.

Um die rechtliche Zulässigkeit der dargelegten Videoüberwachung bewerten zu können, bat der TLfDI den Betreiber der Kamera zunächst um eine Stellungnahme zu den Vorwürfen des Beschwerdeführers. Nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI die zuständige Aufsichtsbehörde für den Datenschutz gemäß § 38 Abs. 1 BDSG. Er kontrolliert die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen

sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht verletzt wird (§ 1 Abs. 1 BDSG).

In diesem Sinne bat der TLfDI insbesondere um Informationen über den Zweck der Videoüberwachung, den Zeitpunkt der Kamerainstallation, die Kameraeinstellungen (Höhe, Erfassungswinkel usw.), Art und Dauer der Datenspeicherung sowie um einen Lageplan und tabellarische Übersichten zu Zeiten der Datenerfassung. Außerdem wollte der TLfDI wissen, ob die Bildaufnahmen mit weiteren Daten verknüpft werden, beispielsweise für einen Personenabgleich.

Nach § 38 Abs. 3 BDSG sind die der Kontrolle des TLfDI unterliegenden Stellen und die mit deren Leitung beauftragten Personen verpflichtet, dem TLfDI die für seine Tätigkeit als Aufsichtsbehörde erbetenen Auskünfte zu erteilen. Dieser Kontrolle unterfallen nicht-öffentliche Stellen Dazu zählen „natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts“, § 2 Abs. 4 BDSG.

Der Kamerabetreiber teilte mit, dass er seit knapp einem Jahr zwei Kameras auf seinem Grundstück installiert hatte, eine Kamera an der Haustür und die andere am Hoftor. Nach eigener Aussage hatte er die Kameras ausschließlich zur Überwachung seines eigenen Grundstücks installiert zur Einlasskontrolle am Hoftor und an seiner Haustür. Beide Kameras erfassten allerdings auch in geringem Umfang öffentlich zugängliche Räume.

Beide Kameras waren weder automatisch schwenkbar noch verfügten sie über eine Zoom-Funktion. Die Kameras waren an zwei Monitore angeschlossen, deren Beleuchtung in der Grundeinstellung ausgeschaltet war. Nur bei Wahrnehmung einer Bewegung wurden die Monitore „aktiviert“ und zeigten die Bilder der Kameras. Somit war ausgeschlossen, dass der Bereich vor dem Hoftor permanent aufgezeichnet wird und es konnten auch keine Bewegungsprofile von zufällig am Hoftor vorbeigehenden Passanten erstellt werden. Zugriff auf die Bilddaten hatten der Kamerabetreiber und dessen Mutter. Die aufgenommenen Bilddaten wurden durch Selbstüberschreibung regelmäßig gelöscht. Als Nachweis für seine Darlegungen hatte der Kamerabetreiber dem TLfDI mehrere Bildaufnahmen mit geöffnetem und ungeöffnetem Hoftor zur Verfügung gestellt. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch nicht-öffentliche Stellen (Unternehmen und Privatpersonen) mittels Datenverarbeitungsanlagen ist im BDSG geregelt. Dies war

durch die Videoüberwachung der Fall. Nach § 4 Abs. 1 BDSG ist eine Videoüberwachung grundsätzlich – wie jeder Umgang mit personenbezogenen Daten – nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung gesetzlich erlaubt ist bzw. angeordnet wird. Anderenfalls ist die Videoüberwachung unzulässig. Eine Einwilligung kam naturgemäß in diesem Fall nicht in Betracht. Als Erlaubnisnorm für die Zulässigkeit war § 6b BDSG heranzuziehen. Danach ist eine Videoüberwachung in einem öffentlich zugänglichen Raum zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist. Dabei dürfen jedoch keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der aufgezeichneten Personen beeinträchtigt werden. Die Kamera umfasste auch den Teil des Gehweges vor der Eingangstür bzw. dem Hoftor und insofern einen kleinen Teil des öffentlichen Raums.

Der TlfDI teilte dem Kamerabetreiber mit, dass für das Tatbestandsmerkmal „öffentlich / nicht-öffentlich zugänglicher Raum“ die Eigentumsverhältnisse am Beobachtungsobjekt keine große Rolle spielen. Nicht-öffentlich zugänglich sind Räume, die nur von einem bestimmten Personenkreis betreten werden können oder dürfen. Allein die bestehende Zugangsmöglichkeit begründet keine Öffentlichkeit, wenn der entgegenstehende Wille des Grundstückseigentümers aus den Umständen erkennbar ist (Scholz in Simitis, BDSG, § 6b, Rn. 42, 43, 48). Im vorliegenden Fall war die Zufahrt zum Grundstück durch ein Hoftor abgeschlossen, auch wenn dieses offen stand. Das Tor ließ erkennen, dass es sich hier um ein Privatgrundstück handelt, das nicht für jedermann zugänglich ist. Doch selbst wenn eine Videoüberwachung zum Zweck der Einlasskontrolle an der eigenen Haustür im Sinne von § 1 Abs. 2 Nr. 3 BDSG durchgeführt wird, kann sie unzulässig sein, falls Anhaltspunkte bestehen, dass schutzwürdige Interessen der „Überwachten“ überwiegen. Im vorliegenden Fall überwachte der Kamerabetreiber neben seinem Privatgrundstück auch den öffentlichen Verkehrsraum. Auf Seiten von Passanten oder Besuchern im öffentlichen Raum bestand daher ein berechtigtes Interesse daran, dass die Aufnahmen von ihnen nicht gespeichert werden.

Nach § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie für ihren Zweck nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen

einer weiteren Speicherung entgegenstehen. Daher hätten die aufgezeichneten Bilddaten spätestens dann gelöscht werden müssen, wenn der Person, die vor der Haustür oder dem Hoftor steht, geöffnet wurde oder wenn sie das Grundstück wieder verlassen hat. Somit verstieß die Speicherung der Aufnahmen gegen das BDSG und war damit rechtswidrig. Für den Zweck der Einlasskontrolle war eine Speicherung der Bilder nämlich nicht erforderlich.

Dementsprechend forderte der TLfDI den Kamerabetreiber dazu auf, eine Alternative zu wählen, die weniger in die Grundrechte auf informationelle Selbstbestimmung von Passanten oder Besuchspersonen eingreift. In diesem Sinne käme eine Videoüberwachung als reines „Monitoring“ infrage, bei dem die Bilder an den Monitor gesendet, jedoch nicht auf einer SD-Karte gespeichert werden.

Weiterhin forderte der TLfDI den Kamerabetreiber dazu auf, eindeutige Hinweisschilder anzubringen, die auf die Videoüberwachung durch den Grundstücksbesitzer hinweisen (§ 6b Abs. 2 BDSG). Passanten oder Besucher müssen einschätzen können, welcher Bereich von den Kameras erfasst wird, damit sie ggf. der Überwachung ausweichen können. Die Kontaktdaten des Kamerabetreibers müssen auf dem Hinweisschild vermerkt sein, damit der Betroffene erkennt, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Das Hinweisschild muss gut sichtbar und in Augenhöhe befestigt werden.

Der Kamerabetreiber bestätigte dem TLfDI schriftlich, dass er die geforderten Maßnahmen betreffend die Bildspeicherung und die Hinweisschilder umgesetzt hatte. Damit erklärte der TLfDI die Videoüberwachung der beiden Kameras als zulässig und teilte dem Beschwerdeführer mit, dass die Videoüberwachung nunmehr mit den Regelungen des BDSG vereinbar ist und er somit nicht in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

In einem öffentlich zugänglichen Raum ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und dabei keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der aufgezeichneten Personen beeinträchtigt werden. Für das Tatbestandsmerkmal „öffentlich / nicht-öffentlich zugänglicher Raum“ sind die Eigentumsverhältnisse am Beobachtungsobjekt jedoch unbeachtlich. Auch in einem nicht-öffentlich zugänglichen

Raum muss die Videoüberwachung erforderlich sein, um den vorgesehenen Zweck zu erreichen. In diesem Sinne ist eine Videoüberwachung zu unterlassen, wenn die damit verknüpfte Speicherung der Bilder gegen § 4 Abs. 1 BDSG verstößt und somit rechtswidrig ist. Gemäß § 6b Abs. 2 BDSG sind in Augenhöhe eindeutige Hinweisschilder auf eine Videoüberwachung anzubringen, die auf die Kameraüberwachung und die dafür verantwortliche Stelle hinweisen.

6.19 Postkartenmotiv „Videokamera“

Auf der Suche nach einem außergewöhnlichen Postkartenmotiv entdeckte ein wachsamer Bürger zwei Videokameras an einem Wohnhaus. Er stellte dies erst im Nachhinein fest, als er die von ihm aufgenommenen Bilder durchsah. Er wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und wollte wissen, ob es überhaupt erlaubt ist, dass er gefilmt wird, wenn er an dem Gebäude vorbeiläuft. Ganz einverstanden war er damit nämlich nicht. Als Nachweis schickte er ein Foto von den Videokameras.

Routinemäßig wandte sich der TLfDI an den Hausbesitzer und bat um Aufklärung der Vorwürfe. Der Hausbesitzer gab zu, dass er der Betreiber der Videokameras ist, allerdings handelt es sich bei den Objekten um funktionsuntüchtige Kameras. In der Vergangenheit musste er viele Schmierereien und Graffiti an seiner Hauswand hinnehmen und um die Vandalen abzuschrecken, hielt er die Lösung für eine gute und kostengünstige Variante. Er war ziemlich frustriert darüber, dass er in der Vergangenheit schon etliche Kosten und Mühe zur Beseitigung der Schmierereien hatte in Kauf nehmen müssen. Die Anzeigen bei der Polizei waren leider erfolglos verlaufen.

Der TLfDI wies den Betreiber der Attrappen darauf hin, dass auch solche Geräte in das Persönlichkeitsrecht Dritter eingreifen können. Der Betreiber nahm Änderungen an deren Ausrichtung vor. Datenschutzrechtlich waren die Attrappen dann nicht mehr zu beanstanden.

Auch für private Haushalte gelten die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren. Zusätzlich können private Haushalte durch Mitbürger über den zivilrechtlichen Weg in die Haftung genommen werden.

6.20 Videoüberwachung eines öffentlichen Raumes der Stadt Rudolstadt durch Privatperson

Eine Thüringer Stadtverwaltung (SV) informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Videoüberwachung durch eine Privatperson. Diese Videoüberwachungsanlage soll nicht nur das Grundstück der Person, sondern auch den Gehweg, also den öffentlich zugänglichen Raum direkt vor dem Grundstück, miteinbeziehen. Der TLfDI wandte sich daraufhin an den vermeintlichen Betreiber der Kamera. Dieser teilte dem TLfDI mit, dass er am besagten Haus (an der gemeldeten Adresse) keine Kamera betreiben würde, er aber an seinem direkten Wohnsitz (in derselben Straße) eine Kamera installiert habe. Er begründete dies mit vergangenen Angriffen auf sein Haus und wollte sich damit schützen. Er sei gegen die Täter vorgegangen und als „Revanche“ wurde sein Privateigentum beschädigt. Weiterhin erklärte er, dass die Aufzeichnungen nur dann zu Beweis Zwecken gespeichert werden, wenn es zu Angriffen kommt. Andernfalls würden die Daten überschrieben werden. Einsicht in diese Aufzeichnungen hätte nur er selbst.

Der TLfDI teilte dem Betreiber daraufhin mit, dass die Aufzeichnung von Videoaufnahmen eine Erhebung und Verarbeitung von personenbezogenen Daten darstellt. Diese ist nach § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Da eine Einwilligung der Betroffenen nicht vorliegt, kommt es darauf an, ob die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig ist, da vorliegend öffentlich zugängliche Räume erfasst wurden. Nach dieser Vorschrift ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Hausrecht umfasst die Befugnis, grundsätzlich frei darüber zu entscheiden, wem der Zutritt zu einer Örtlichkeit gestattet und wem er verwehrt wird. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn

eine tatsächliche Gefahrenlage nachgewiesen werden kann. Hier sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit, nachzuweisen. Da die Videoüberwachungsanlage auch den öffentlichen Raum, sprich den Fußweg, miterfasste, bestehen Anhaltspunkte, dass die schutzwürdigen Interessen der betroffenen Personen nicht gewahrt sind. Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mithilfe von Kameras beobachtet oder aufgezeichnet wird. Zudem sieht sich der Einzelne einem permanenten Überwachungsdruck ausgesetzt, der eine Beeinträchtigung des Persönlichkeitsrechts darstellt. Nach § 38 Abs. 5 Satz 1 BDSG kann der TLfDI als Aufsichtsbehörde zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der TLfDI bat den Betreiber um Nachweise der tatsächlichen Gefahrenlage durch sorgfältige Dokumentation der Ereignisse.

Gleichzeitig wandte sich der TLfDI an die SV und teilte dieser mit, dass es an der gemeldeten Adresse keine Videoüberwachungsanlage durch den vermeintlichen Eigentümer geben würde, sondern an seinem Wohnsitz in derselben Straße. Aufgrund der örtlichen Nähe zur streitgegenständlichen Videoüberwachungsanlage wollte der TLfDI von der SV wissen, ob die Kamera zwischenzeitlich entfernt worden ist und bat Bilder der noch vorhandenen Kamera zu übersenden. Kurz darauf teilte die SV mit, dass die Kamera entfernt wurde.

Damit sah der TLfDI das Verfahren als erledigt an und teilte dies dem Betreiber der Videokameras mit.

Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz, § 38 Abs. 6 BDSG. Nach § 38 Abs. 1 BDSG kontrolliert der TLfDI die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 4 Abs. 1 Satz 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur

zulässig, wenn der Betroffene eingewilligt hat oder dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt. Wenn eine Einwilligung der Betroffenen nicht vorliegt, kommt es darauf an, ob die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig ist, sofern, wie in diesem Fall, öffentlich zugängliche Bereiche videoüberwacht werden. Nach dieser Vorschrift ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Hausrecht umfasst die Befugnis, grundsätzlich frei darüber zu entscheiden, wem der Zutritt zu einer Örtlichkeit gestattet und wem er verwehrt wird. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein.

6.21 Videoüberwachung nicht über den Maschendrahtzaun hinaus?

Aufgrund eines Nachbarschaftsstreits um einen versetzten Maschendrahtzaun informierte sich eine sog. Teilbesitzerin des Zauns, ob eine Videoüberwachung auf ihrem Grundstück aus datenschutzrechtlicher Sicht zulässig ist. Hintergrund sei, dass es vermehrt zu Streitereien zwischen ihr und dem Nachbarn gekommen ist, was das unbefugte Versetzen des Maschendrahtzauns auf den Grundstücksgrenzen betraf. Auch würden andere Anwohner an ihrem Maschendrahtzaun diversen Vandalismus betreiben. Ihr Anliegen war es nun, eine Videoüberwachungsanlage zu installieren, damit sie zum einen mitbekommt, wenn der Nachbar wieder unbefugt den Maschendrahtzaun auf ihr Grundstück versetzen sollte, und zum anderen, damit sie erfährt, wenn die Kinder von Anwohnern wiederholt diverse Gegenstände am Zaun entsorgen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) konnte hier nur allgemein auf ihre Anfrage antworten, da sie noch keine Videoüberwachung installiert hatte. Des Weiteren wurde im geschilderten Sachverhalt davon ausgegangen, dass die Betroffene die Videoüberwachung lediglich auf ihrem Grundstück betreiben und der Aufnahmebereich nicht auf Nachbargrundstücke oder angrenzende, öffentlich zugängliche Bereiche, wie Straßen oder Gehwege, ausgerichtet sein wird.

Allgemein wurde ausgeführt: Bei einer Videoüberwachung werden aufgrund der Beobachtung personenbezogene Daten erhoben und, sofern die Aufnahmen aufgezeichnet werden, gleichzeitig verarbeitet. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Es bleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die die Videoüberwachung erlaubt. Eine Überwachung im privaten Bereich ist nur unter bestimmten Umständen rechtlich zulässig. Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Handelt es sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher zulässig. Sollte die Videoüberwachung nicht die Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG erfüllen, ist für die nicht-öffentliche Stelle die maßgebliche Erlaubnisnorm der § 6b BDSG. Hier hat der Gesetzgeber im § 6b Abs. 1 Nr. 2 bis 3 BDSG klar geregelt, welche Voraussetzungen erfüllt sein müssen, damit die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch nicht-öffentliche Stellen zulässig ist. § 6b Abs. 1 Nr. 1 BDSG ist hier nicht zutreffend, da es um die Aufgabenerfüllung öffentlicher Stellen geht. Im oben genannten Einzelfall ist zunächst die Variante des § 6b Abs. 1 Nr. 2 BDSG – zur Wahrung des Hausrechts – zu prüfen. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen endet. Wer außer seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. In diesem Fall wäre dann der § 6b Abs. 1 Nr. 3 BDSG nach seiner Zulässigkeit im Einzelfall zu prüfen. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwa-

chungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mit überwacht werden. Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die sich dort befindlichen Personen erfasst werden können. Auch lässt die Rechtsprechung (vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter aufgenommen wird.

Hinzu kommt noch, sollte die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig sein, dass die Videoüberwachungsanlage eine automatisierte Verarbeitung nach dem BDSG und diese meldepflichtig nach § 4d BDSG ist. Nicht-öffentliche Stellen, die Videoüberwachungsanlagen einsetzen, sind verpflichtet, dies dem TLfDI als zuständiger Aufsichtsbehörde zu melden, wenn sie keinen betrieblichen Datenschutzbeauftragten haben. Der oben genannte Fall stellt eine solche Meldepflicht dar. Hierzu gibt es auch ein Urteil vom Oberverwaltungsgericht (OVG) Saarland vom 14. September 2017. Genauereres dazu kann auch in der Pressemitteilung vom TLfDI „Meldepflicht für (Wild-)Kameras bestätigt!“ (siehe Anlage 5) nachgelesen werden. Bei allgemeinen Anfragen verweist der TLfDI immer auf die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises, in der die Grundsätze zulässiger Videoüberwachung aufgeführt sind. Diese Orientierungshilfe stellt der TLfDI auf seiner Website (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_nicht-ffentliche-stellen.pdf) zur Verfügung.



Ob die Betroffene letztendlich Videoüberwachung auf ihrem Grundstück – gestützt auf ihr Hausrecht – betreibt, ist dem TLfDI nicht bekannt.

Es empfiehlt sich immer, bevor Videoüberwachungsanlagen installiert werden – egal an welchem Standort –, den TLfDI mit einzuschalten und das Vorhaben aus datenschutzrechtlicher Sicht prüfen zu lassen.

6.22 Videoüberwachung auf eigenem Grundstück zulässig?

Ein Anwohner fühlte sich durch eine am Gebäude seines Nachbarn angebrachte Kamera so sehr in seinem Persönlichkeitsrecht beeinträchtigt, dass er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte. Der Anwohner vermutete, dass die Kamera so ausgerichtet war, dass diese womöglich seinen Eingangsbereich, Teile des Grundstücks und auch des öffentlichen Bereichs filmte.

Der TLfDI nahm die Beschwerde zum Anlass und erkundigte sich beim Betreiber der Videokamera – sprich beim Nachbarn. Der Betreiber erhielt vom TLfDI – wie es üblich ist – einen umfangreichen Fragenkatalog zu seiner installierten Kamera. Der Betreiber war kooperationsbereit und arbeitete dem TLfDI die benötigten Auskünfte zu dem Fragenkatalog zu. Er skizzierte in Lageplänen den Standort der installierten Kamera. Jedoch stellte sich bei der Beantwortung des Fragenkatalogs heraus, dass es sich nicht um eine funktionstüchtige Kamera handelte, sondern um eine Kameraattrappe. Die Kamera war oberhalb auf der Eingangstür angebracht, ausgerichtet auf den privaten Hauseingang und Vorgarten des Betreibers. Die Attrappe war ausschließlich auf das Grundstück des Besitzers ausgerichtet. Bei Hauseingängen ist zu beachten, dass es sich dabei regelmäßig um öffentlich zugänglichen Raum handelt. Innerhalb solcher Bereiche ist die Videoüberwachung nur nach Maßgabe von § 6b BDSG zulässig. Außerdem ist auf die Videoüberwachung hinzuweisen. Im Ergebnis war die Attrappe datenschutzrechtlich nicht zu beanstanden.

Das Ergebnis der datenschutzrechtlichen Prüfung wurde auch dem Beschwerdeführer – also den Anwohner, der sich an den TLfDI gewandt hatte – mitgeteilt, jedoch war das Ergebnis dessen Unverständnis. Der Bitte einer nochmaligen Prüfung ist der TLfDI nicht nachgegangen, da hier die Rechtslage eindeutig war.

Die Beurteilung von datenschutzrechtswidrig oder datenschutzzulässig installierten Kameras ist sehr komplex, da die rechtliche Einordnung von unterschiedlichen Umständen des Einzelfalls abhängig ist. Unter Umständen kann auch eine installierte Kamera aus datenschutzrechtlicher Sicht zulässig sein; leider auch zum Unverständnis anderer.

6.23 Achtung: Im Vogelhaus nistet eine Kamera! – Videogaga 8

Ein Bürger wandte sich mit einer E-Mail an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er fühlte sich seit geraumer Zeit durch seinen Nachbarn beobachtet und in seiner Privatsphäre gestört. Besagter Nachbar hatte, getarnt durch ein Vogelhaus, eine Überwachungskamera installiert. Die Rückfrage bei dem besagten Nachbarn ergab folgenden Sachverhalt: Die „nistende“ Kamera war über Funk mit einem Monitor verbunden, der im Vorbau des Einfamilienhauses installiert war. Dieser gab nur Bilder wieder, wenn die Klingel am Gartentor betätigt wurde. Die Kamera diente zur Erkennung der Personen, die am Eingang zum Grundstück klingelten. Das Eingangstor befand sich etwa 20 Meter vom Hauseingang entfernt und war vom eigentlichen Hauseingang nicht einsehbar. Das Vogelhaus, in dem die Kamera „nistete“, war in einer Entfernung von sieben Metern zur Grundstücksgrenze aufgestellt. Die Kamera war nicht schwenkbar und verfügte über keine Zoomfunktion. Der Monitor zur Kamera war von 8:00 bis 21:00 Uhr eingeschaltet. Es erfolgte keine Aufzeichnung und keine Speicherung der Bilder. Weiterhin gab es keinen Anschluss der Kamera an einen Computer. Einblick auf den Monitor hatten nur der Nachbar und seine Frau.

Die von ihm vorgenommene Videoüberwachung wurde nach Auswertung der vorliegenden Informationen vom TLfDI wie folgt bewertet:

Das Bundesdatenschutzgesetz (BDSG) verfolgt den Zweck, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, § 1 Abs. 1 BDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen, Privatpersonen) wird durch das BDSG geregelt, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben. Der TLfDI hat hingegen keine Zuständigkeit, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13 ist diese Regelung allerdings eng auszulegen. Entscheidend sei, ob auch Personen von der Videokamera erfasst werden können,

die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen videoüberwacht werden, die nicht dem eigenen familiären Bereich zuzuordnen sind. Der Aufnahmebereich der hier kontrollierten Kamera erfasste zum Teil die Straße vor dem Grundstück des Videobetreibers. Da sich der Aufnahmebereich über sein eigenes Grundstück hinaus erstreckte, hatte er keinen Einfluss darauf, wer sich in diesen Bereich hinein bewegte. Es bestand die Möglichkeit, dass Dritte in den Aufnahmebereich der Kamera gelangen konnten, so etwa Spaziergänger, Nachbarn oder Besucher. Nach § 4 Abs. 1 BDSG ist eine Videoüberwachung grundsätzlich wie jeder Umgang mit personenbezogenen Daten nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung durch eine gesetzliche Vorschrift erlaubt wird. Ist keine der beiden Voraussetzungen gegeben, so ist die Videoüberwachung unzulässig. Eine Einwilligung ist im Rahmen des Einsatzes einer Videoüberwachung schwer umsetzbar. Als Erlaubnisnorm kommt vorliegend nur der § 6b BDSG infrage. Demnach ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Die vom besagten Nachbarn angebrachte Videoüberwachung sollte zu Beobachtungszwecken in Form eines verlängerten Auges als präventives Mittel dienen, um zu sehen, wer bei ihm am Gartentor klingelte.

Besagter Nachbar gab an, dass die Kamera installiert wurde, damit seine Frau auf dem Monitor frühzeitig erkennen konnte, ob ungebetene Gäste den Zutritt zu ihrem Grundstück erzwingen wollten und entscheiden konnte, ob sie die Haustür öffnete oder eben nicht.

Vor dem Einsatz eines Videoüberwachungssystems ist zu überprüfen, ob es tatsächlich für den festgelegten Zweck geeignet und erforderlich ist, § 6b BDSG. Die Erforderlichkeit einer Videoüberwachungsanlage kann nur dann bejaht werden, wenn keine gleich wirkenden Mittel in Betracht kommen, die weniger stark in das Recht auf informationelle Selbstbestimmung Dritter eingreifen. Zu dem vom Videobetreiber verfolgten Zweck stellt sich keine mögliche Alternative dar, die weniger in Rechte Dritter eingreift. Zumal er die Videoüberwachung in den o. g. eingeschränkten Zeiten durchführte. Selbst

wenn eine Erforderlichkeit der Videokamera gegeben ist, kann sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Erfassungsbereich der Kamera ging über das Grundstück des Nachbarn hinaus. Auf den von der Kamera aufgenommenen Bildern war die Straße vor seinem Grundstück ersichtlich. Wie oben bereits dargestellt, hatte er keinen Einfluss darauf, wer sich in diesen Bereich hinein bewegte. Dies stellte einen Eingriff in das Persönlichkeitsrecht der Passanten und/oder seiner Nachbarn dar. In dem Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 mit dem Aktenzeichen 16 C 427/02 wurde entschieden, die Videoüberwachung mittels der Videokamerasysteme (Anzahl: drei) im Bereich des Arkadenganges der betroffenen Straße in Berlin zu unterlassen, soweit diese über einen 1 Meter breiten Streifen entlang der Schaufensterseite sowie einen 1 Meter breiten Streifen links und rechts der Arkadensäulen einschließlich des darüber befindlichen Luftraums hinausgeht.

Es überwiegen die schutzwürdigen Interessen Dritter am Ausschluss einer Videoüberwachung die Interessen des Nachbarn, zu sehen, wer bei ihm geklingelt hat.

Nach Einschreiten des TLfDI wurde die Kamera entsprechend diesen Vorgaben ausgerichtet.

Ferner fehlte ein eindeutiges Hinweisschild, welches den Umstand der Videoüberwachung sowie die verantwortliche Stelle erkennen lässt, § 6b Abs. 2 BDSG. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Bei Benennung der verantwortlichen Stelle auf dem Hinweisschild ist entscheidend, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher war der besagte Nachbar als verantwortliche Stelle verpflichtet, seine Kontaktdaten explizit auf dem Hinweisschild zu benennen. Bei der Anbringung des Hinweisschildes war ebenfalls darauf zu achten, dass dieses gut sichtbar war und in Augenhöhe befestigt wurde.

Der TLfDI kam zum Ergebnis, dass die „nistende“ Kamera erst mit den datenschutzrechtlichen Bestimmungen des Bundesdatenschutzgesetzes vereinbar war, nachdem der Blickwinkel der Kamera derart verändert wurde, dass der Erfassungsbereich höchstens einen Meter entlang der Grundstücksgrenze verlief. Darüber hinaus musste der

Nachbar ein Hinweisschild anbringen, dass den o. g. Forderungen aus § 6 Abs. 2 BDSG genüge.

Eine neuerliche Prüfung durch den TLfDI ergab, dass die Auflagen durch den besagten Nachbarn erfüllt wurden. Der TLfDI konnte keinen datenschutzrechtlichen Verstoß mehr feststellen. Eine Aufzeichnung von öffentlich zugänglichen Räumen vor der Grundstücksgrenze fand, nach Veränderung des Standorts des Vogelhäuschens nebst der Kamera nicht mehr statt. Ein Eingriff in das Recht auf informationelle Selbstbestimmung in rechtswidriger Art und Weise lag nun nicht mehr vor.

Grundsätzlich ist die Videoüberwachung auf dem eigenen und allein genutzten Grundstück zulässig. Die Beobachtungsbefugnis des Hausrechtsinhabers endet jedoch an der Grundstücksgrenze. Eine darüber hinausgehende Beobachtung in den öffentlichen Raum ist seit der Entscheidung des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003, Az. 16 C 427/02 lediglich bis zu einem Meter über die Grundstücksgrenze hinaus zulässig. Darüber hinaus darf eine Videoüberwachung in den öffentlichen Raum nicht erfolgen.

6.24 Dome

Eine an einer Garage befestigte Dome-Kamera war ein Fall für den Datenschutzbeauftragten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt darüber Kenntnis, dass in einem Ort in Thüringen ein Hausbewohner eine Dome-Kamera an seiner Garagenwand installiert hatte. Bei der Dome-Kamera konnte man allerdings nicht die Ausrichtung erkennen, da die Kamera von einem runden schwarzen Gehäuse umhüllt war.

Bei der Beurteilung der Zulässigkeit von Videokameras, die an Wohnhäusern bzw. Garagen angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Es verbleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn es handelt sich um private oder familiäre Aufnahmen, dann ist das Bundesdatenschutzgesetz nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG). Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13 ist diese Regelung allerdings eng auszulegen. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönli-

chen oder familiären Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn öffentlich zugängliche Räume beobachtet werden, die von Personen frequentiert werden können, die mit dem Videobetreiber nicht in enger familiärer Beziehung stehen. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher oftmals schon allein wegen der Nichtanwendbarkeit des BDSG durch die Aufsichtsbehörde nicht bewertbar. Spätestens an den Grundstücksgrenzen endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel.

Soweit mit einer Videokamera neben dem eigenen Grundstück auch der öffentlich zugängliche Raum in der Umgebung wie Straßen, Gehwege oder Parkplätze und die dort befindlichen Personen miterfasst werden können, ist maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage § 6b BDSG. Danach ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen.

In einem weiteren Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2013 Az.: 16 C 427/02 wurde entschieden, dass eine Videoüberwachungsanlage einen 1 Meter breiten Streifen entlang der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen dürfe, wenn dies für Zwecke des Hausrechts erforderlich ist. Voraussetzung hierfür ist allerdings, dass durch geeignete Maßnahmen nach § 6b Abs. 2 BDSG auf die Videoüberwachung hingewiesen wird und Passanten oder Nachbarn gefahrlos einer Bildaufnahme ausweichen können.

Die Erfüllung der gesetzlichen Voraussetzungen konnte der Betreiber der Dome-Kamera glaubhaft nachweisen und der TLfDI bewertete die Dome-Kamera als rechtlich zulässig.

Videokameras sind heutzutage leider allgegenwärtig. Im unternehmerischen Bereich als auch in privaten Haushalten sind sie auf dem Vormarsch. Dabei gelten auch für private Haushalte die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren. Noch dazu setzt man sich der Gefahr

aus, dass man von seinen Mitbürgern zivilrechtlich in die Haftung genommen wird.

6.25 Wanderer zeigen Bein: Videogaga 9

Im Mai 2016 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine E-Mail der Verwaltung eines Naturparks in Thüringen. Der TLfDI musste prüfen, ob es zulässig sei, Kameras am Wanderweg zu installieren. Die Kameras sollten einem Studenten, der im Zuge seiner Bachelorarbeit für die Betreuung und Auswertung der Zählerstationen entlang des Leine-Werra-Wanderwegs verantwortlich war, dazu dienen, die Anzahl der Besucher zu erfassen.

Der TLfDI stellte folgende Bedingungen, damit der Installation keine datenschutzrechtlichen Bedenken entgegenstanden: Die Kameras durften keine personenbezogenen Daten erfassen, d. h. die Identifizierung der Personen durfte nicht möglich sein. Der Student erklärte, dass die Kameras so bodennah installiert werden könnten, dass sie nicht sichtbar wären und nur die Beine der Spaziergänger erfasst werden würden. Durch diese bodennahe Bildperspektive war sichergestellt, dass keine personenbezogenen Daten erfasst wurden. Das sollte auch noch dadurch unterstützt werden, dass eine grobe Bildauflösung zu wählen war.

Nachdem der Student diese Informationen erhalten hatte, wollte er die Kameras wie geplant aufstellen, jedoch musste er feststellen, dass seine Kameras nicht für diesen Einsatzzweck geeignet waren. Aus Kosten- und Zeitgründen hat er sich entschlossen, eine manuelle Besucherzählung durchzuführen. Die Kameras kamen nicht zum Einsatz.

Aus datenschutzrechtlicher Sicht ist ein Einsatz der Kameras auf Wanderwegen zum alleinigen Zweck der Überprüfung der an Zählerstationen gemessenen Besucherzahlen dann unbedenklich, wenn dadurch keine personenbezogenen Daten erhoben werden. Dafür ist gesorgt, wenn eine grobe Bildauflösung gewählt wird und die Kamera nur einen Ausschnitt der Beine der Wanderer erfasst.

6.26 Kamera im Mehrfamilienhaus beliebt: Videogaga 10

Ein Ehepaar wandte sich mit einer allgemeinen Anfrage an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass ihr Vermieter in ihrem Mietshaus mit mehreren Mietparteien eine Kamera installiert hat und wollte wissen, ob dies zulässig ist und der Zustimmung durch die Mieter bedarf. Die Überwachungsanlage befindet sich im Inneren des Hauses. Der Vermieter hat die Mieter nicht über das Bildaufnahmegerät informiert und dies ohne deren Zustimmung angebracht. Die Betroffenen wollten auch wissen, welche Vorschriften für die Auswertung der Daten existieren und wie Verstöße sanktioniert werden.

Der TLfDI teilte den Anfragenden mit, dass grundsätzlich eine Videoüberwachung in einem Mietshaus zulässig ist, wenn die gesetzlichen Voraussetzungen dafür vorliegen. Dies lässt sich nicht pauschal, sondern immer nur im Einzelfall feststellen. Einer Zustimmung der Mieter bedarf es in diesem Fall nicht. Für die datenschutzrechtliche Bewertung ist bedeutsam, ob die Kamera öffentlich zugänglichlichen Raum aufnimmt, in diesem Fall wäre § 6b Bundesdatenschutzgesetz (BDSG) einschlägig. Handelt es sich hingegen um einen nicht-öffentlich zugänglichlichen Bereich, wie bei dem Innenbereich eines Mehrfamilienhauses, greift die Bestimmung des § 28 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel



für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf veröffentlicht ist. Diese Orientierungshilfe ließ der TLfDI dem Ehepaar zukommen.

Grundsätzlich stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Außerdem haben die Eheleute gegenüber dem

Betreiber der Videoüberwachung ein Auskunftsrecht nach § 34 Abs. 1 BDSG. Aufgrund des nicht genau beschriebenen Sachverhalts des Ehepaars ließ sich grundsätzlich nicht sagen, ob es sich hier um einen Verstoß handelt. Die Beschwerdeführer haben sich nach der Information durch den TLfDI nicht mehr gemeldet.

Sollten Bewohner eines Mietshauses feststellen, dass dort eine Videoüberwachung vorliegt, können sie sich an den TLfDI wenden. Genauere Angaben zu den Anforderungen an eine zulässige Videoüberwachung finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter <https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v-durch-nicht-ffentliche-stellen.pdf> veröffentlicht ist.



6.27 Störung des Hausfriedens durch Videoüberwachung – Videogaga 11

Ein Mieter beschwerte sich bei seiner Hausverwaltung, da in dem Mietshaus Kameras angebracht wurden, die unter anderem auf die Eingangstür des Hauses gerichtet waren. Er verlangte eine schriftliche Begründung der Maßnahme von der Hausverwaltung. Die Hausverwaltung begründete die Kameraüberwachung damit, dass sie wiederholt Sachbeschädigungen in dem Haus feststellen musste. Um die Werte zu erhalten und zukünftige Straftaten zu verhindern, habe der Eigentümer, eine Wohnungsgesellschaft, entschieden, den Eingangsbereich überwachen zu lassen. Laut Schreiben an den Mieter werden die gesammelten Daten in regelmäßigen Abständen gesichtet, und, wenn darauf keine Straftat erkennbar ist, gelöscht. Der Beschwerdeführer bemerkte daraufhin, dass die Bewohner des Hauses nicht nach einer Zustimmung gefragt wurden und er bat den Vermieter, die Verhältnismäßigkeit der Überwachungsmaßnahme zu prüfen.

Der Beschwerdeführer wandte sich zudem an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), damit dieser die Angelegenheit datenschutzrechtlich prüfen konnte.

Der TLfDI richtete dann eine Nachricht an die Hausverwaltung, um Auskunft nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) über die angebrachten Kameras zu erhalten. Außerdem wies er als zuständige Aufsichtsbehörde darauf hin, dass nach § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine solche Einwilligung liegt nicht vor, im Gegenteil, der Beschwerdeführer hatte ein Beschwerdeschreiben verfasst, in dem mehrere Mieter gegen die Videoüberwachung unterzeichnet hatten.

Auf das Auskunftersuchen erhielt der TLfDI die Antwort, dass es sich lediglich um Kameraattrappen handele, allerdings demnächst aktive Kameras angeschafft werden sollen. Auch wenn es sich um Kameraattrappen handelte, bat der TLfDI die Hausverwaltung darzulegen, zu welchem Zweck die Attrappen angebracht wurden und welchen vermeintlichen Aufnahmebereich sie haben.

Die Hausverwaltung erklärte dem TLfDI, dass nicht sie, sondern die Eigentümergemeinschaft den Beschluss gefasst hatte, dass in dem Haus eine Videoüberwachung stattfinden solle. Der TLfDI erläuterte, dass nach § 3 Abs. 7 BDSG die verantwortliche Stelle jede Person oder Stelle ist, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Sollte die Eigentümergemeinschaft also die Hausverwaltung mit der Videoüberwachung beauftragt haben, müssten sie einen Vertrag nach § 11 BDSG über die Datenverarbeitung im Auftrag geschlossen haben. Dieser Vertrag müsste dann dem TLfDI vorge-



legt werden. Auf die Nachfrage, wie man eine Überwachung durchführen könne, ohne gegen das geltende Recht zu verstoßen, fügte der TLfDI die „Orientierungshilfe Videoüberwachung bei nicht-öffentlichen Stellen“ (https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v_-durch-nicht-ffentliche-stellen.pdf) dem Schreiben bei.

Diese wurde von den Datenschutzaufsichtsbehörden im Düsseldorfer Kreis erarbeitet, um den privaten Betreibern von Videoüberwa-

chungsanlagen das nötige Wissen hinsichtlich der datenschutzrechtlichen Anforderungen zu übermitteln. Sie soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Daraus ergibt sich auch, dass ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage im Sinne von § 6b Abs. 1 Nr. 3 BDSG von ideeller, wirtschaftlicher oder rechtlicher Natur sein kann. Soll die Videoüberwachung wie im vorliegenden Fall dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Dafür forderte der TLfDI konkrete Nachweise, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit.

Die Hausverwaltung bestätigte nun explizit, dass der Betreiber der geplanten Videoüberwachung die durch die Hausverwaltung vertretene Wohnungseigentümergeinschaft ist. Außerdem erklärte sie, dass es in den letzten Jahren häufig zu Vandalismus und versuchten Wohnungseinbrüchen gekommen ist. Laut der Hausverwaltung habe die Wohnungseigentümergeinschaft sich unter Abwägung der verschiedenen Interessen entschieden, den Bereich der Hauseingangstür und den Bereich der Tür des Fahrstuhls mittels Kameras zu überwachen bzw. zunächst dort Attrappen anzubringen. Erste Erfolge seien bereits erkennbar: So war nach der Anbringung der Kameras kein Vandalismus mehr erkennbar. Geplant sei daher, diese Bereiche durch aktive Kameras dauerhaft zu überwachen. Die dabei erhobenen Daten sollen für eine Dauer von vier bis sieben Tagen in einem verschlossenen Raum digital gespeichert werden und sich fortlaufend überschreiben. Die Auswertung der Daten solle durch einen bewohnenden Eigentümer erfolgen, da dieser Polizist und dadurch nach Ansicht der Hausverwaltung ausreichend dafür qualifiziert ist. Mit diesem Schreiben erhielt der TLfDI einen Lageplan der angebrachten Kameras und eine Stellungnahme des Eigentümers, der die Daten auswerten soll.

Die Hausverwaltung ließ sich nun in der Angelegenheit durch einen Anwalt vertreten, der auch auf die Fragen des Auskunftersuchens antwortete.

Der TLfDI beschloss, eine Kontrolle vor Ort durchzuführen, dafür verabedete er sich mit dem Beschwerdeführer. Während der Kontrolle war ersichtlich, dass zwei Wohnungseingangstüren in den

Beobachtungsbereich fielen. Es handelte sich hier um sogenannte Wildkameras, die bei Bewegungen im Erfassungsbereich Einzelbilder erstellen, das heißt auch, dass dies grundsätzlich funktionsfähige Kameras sind, also keine Attrappen. Außerdem stellte der TLfDI fest, dass sich auch an der Außenwand des Gebäudes eine Kamera befand, die ausschließlich auf den öffentlich zugänglichen Raum gerichtet waren.

Der TLfDI teilte dem Beschwerdeführer und der Eigentümergemeinschaft mit, dass die Kameras in und an dem Mietobjekt nicht mit dem geltenden Datenschutzrecht vereinbar sind. Zwar wurden von der verantwortlichen Stelle Gründe für die Videoüberwachung angeführt, die berechnigte Interessen nach § 28 Abs. 1 Nr. 2 BDSG begründen können. Allerdings liegen die Vorfälle schon einige Zeit zurück. Außerdem besteht Grund zu der Annahme, dass im konkreten Fall das schutzwürdige Interesse der Mieter des Hauses an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Jeder Besucher des Hauses wird potenziell von der Kamera erfasst, wenn er dieses betritt. Passiert er die Treppe, wird er ebenfalls aufgenommen. Damit liegt eine möglicherweise permanente Überwachung vor, der eine betroffene Person nicht ausweichen kann, da die Bewohner auch bei der dauerhaften Überwachung von Eingängen auf die Nutzung des überwachten Bereichs angewiesen sind. Damit ist eine Rundumüberwachung des sozialen Lebens in dem Miethaus verbunden, die nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Verschmutzungen oder Vandalismus verhindern möchte.

Darauf nahm der Anwalt der Hauseigentümerschaft Bezug und listete die Schäden auf, die in den letzten Jahren durch Vandalismus entstanden sind, zudem nannte er die veranlassten strafrechtlichen Ermittlungsverfahren. Wenig später teilte der Beschwerdeführer dem TLfDI mit, dass die angebrachten Kameras entfernt wurden. Der TLfDI erhielt auch ein Schreiben des Anwaltes; dort wurde angeführt, dass, nachdem die Kameras ihren Zweck erfüllt hatten und keine weiteren Delikte auftraten, diese, um den Hausfrieden zu wahren, demontiert wurden.

Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nach § 28 BDSG richtet. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfa-

milienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum und im Fahrstuhl selbst, einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Eine Rundumüberwachung des sozialen Lebens kann nicht dadurch gerechtfertigt werden, dass der Vermieter mit der Überwachung Schmierereien, Verschmutzungen oder geringfügigen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

6.28 Rund um die Uhr ein Blick ins Unternehmen – Videoga- ga 12

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass in einem Thüringer Unternehmen vor Kurzem in der Produktionshalle, dem Lagerbereich, dem Bürotrakt und im Außenbereich Videokameras installiert worden seien. Die Kameras würden sich drehen und schwenken im Innenbereich auch zu den Aufenthaltsräumen und den Mitarbeitertoiletten. Die Vorgesetzten könnten die Mitarbeiter jederzeit über ihren Bildschirm beobachten. Es deute alles darauf hin, dass die Kameras über eine Zoomfunktion verfügten und akustische Aufnahmen anfertigten. An den Türen seien Aufkleber angebracht worden, die auf die Videoüberwachung hinwiesen. Ansonsten sei den Mitarbeitern nichts Konkretes zur Videoüberwachung mitgeteilt worden. Ein Datenschutzbeauftragter sei nicht bestellt, ein Betriebsrat existiere auch nicht.

Der TLfDI wandte sich mit einem Auskunftersuchen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Geschäftsführung des Unternehmens und bat um nähere Auskunft. Die Geschäftsleitung führte aus, man habe eine Videoüberwachungsanlage mit insgesamt vier Kameras installiert. Beweggrund dafür sei die Abgelegенheit des Firmengeländes am Ende eines neu erschlossenen Gewerbegebiets gewesen. Immerhin lägen circa 100 m zwischen dem Unternehmen und anderen Gewerbeobjekten bzw. Wohnhäusern. Da das Firmengebäude nur zu den täglichen Geschäftszeiten besetzt sei, keine Schicht- oder Wochenendarbeit stattfinde und kein Werkchutz vorhanden sei, wollte man einen möglichen Einbruch, aber auch Schäden durch Wasser, Sturm und Hagel etwa zu Nachtzeiten und am Wochenende zeitnah bemerken können. Zu diesem Zweck sollten es die vier installierten Netzwerkkameras in der Fertigungs-

halle, im Lager, im Flur der Büroräume und im Außenbereich dem Geschäftsführer bequem ermöglichen, von zu Hause aus über einen Web-Browser unter Nutzung des Internets den Zustand der Zugangs-türen, der Hallentore, des Zufahrttores sowie von Teilbereichen der Innenräume auf unbefugten Zutritt live zu überprüfen. Auf eine Aufzeichnung der Aufnahmen habe man allerdings aus Speicher- und Netzkapazitätsgründen verzichtet. Man prüfe noch die technischen Möglichkeiten, die Kameras zeitgesteuert nur in den Abend- bzw. Nachtstunden sowie am Wochenende zu betreiben, um eine eventuelle Überwachung der Mitarbeiter auszuschließen.

Eine Videoüberwachung, die in nicht-öffentlich zugänglichen Räumen stattfindet und nicht im Zusammenhang mit dem Beschäftigungsverhältnis steht, ist an den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu messen. Der Einsatz von Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. Ausnahmsweise können Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Fokus der Überwachung steht und nicht permanent erfasst wird. Dabei ist vorab zu prüfen, ob weniger einschneidende Mittel in Betracht kommen und ob die Videoüberwachung für den dargelegten Zweck auch geeignet ist. Insbesondere die Geeignetheit warf weitere Fragen auf. Kann der Geschäftsführer über sein Handy oder seinen PC zu Hause, wenn er nicht permanent den Livestream beobachtet, denn tatsächlich feststellen, dass ein Tor oder eine Tür unbefugt geöffnet wurde?

Nach entsprechenden Arbeiten wurde berichtet, man habe die Anlage neu konfiguriert. Hauptaugenmerk sind nun die Zugangstüren. Danach übertragen die Kameras, die schwenken und zoomen können, nur noch außerhalb der Geschäftszeiten die Bilder aus menschenleeren Räumen. Bevor die ersten Mitarbeiter morgens eintreffen, werden die Kameras automatisch abgeschaltet. Zusätzlich hat man die Hinweise auf die Videoüberwachung konkretisiert und auch den Mitarbeitern die Informationen über die konkreten Festlegungen und Modalitäten zukommen lassen.

Da das Unternehmen keinen Datenschutzbeauftragten nach § 4f BDSG bestellt hatte, war die Videoüberwachung als Verfahren automatisierter Verarbeitung vor ihrer Inbetriebnahme gemäß § 4d Abs. 1 BDSG dem TLfDI als Datenschutzaufsicht zu melden. Hierfür stellt der TLfDI auf seiner Homepage entsprechende Formulare

und Muster zur Verfügung. Die Meldung zum Register ist zwischenzeitlich erfolgt.

Die Videoüberwachung menschenleerer Räume kann zur Wahrung berechtigter Interessen aus Gründen der Sicherheit zulässig sein. Auch wenn letztendlich ausgeschlossen werden kann, dass Mitarbeiter erfasst werden, sollten sie dennoch eine Information über die Festlegungen erhalten. Sichtbare Kameras, auch wenn sie nicht eingeschaltet sind, erzeugen ebenso wie laufende Kameras insbesondere auf Mitarbeiter einen Überwachungsdruck, den man durch entsprechende Information minimieren kann.

6.29 Campingplatzatmosphäre – Videogaga 13

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um die Prüfung der rechtlichen Zulässigkeit einer Videoüberwachungsanlage. Die Anlage befand sich an einer Gaststätte auf einem Campingplatz. Eigentümer der Gaststätte war die Stadt, aber betrieben wurde sie von einem privaten Pächter. Vor etwa zwei Jahren installierte der Betreiber, nach Informationen des Beschwerdeführers, sechs Kameras an den Außenwänden der Immobilie, um das Umfeld des Gebäudes zu überwachen. Die Campinggäste fühlten sich durch die Kameras überwacht. Der Beschwerdeführer sendete als Anlage Bilder der Außenwand, um die Standorte der Kameras zu dokumentieren. An dem gesamten Gebäude befindet sich nur ein Hinweis darauf, dass eine Videoüberwachung stattfindet. Der Beschwerdeführer informierte den TLfDI ebenfalls darüber, dass eine Aufzeichnung der Aufnahmen stattfände. Außerdem sei kein Grund für die Überwachung ersichtlich, da in den letzten Jahrzehnten keine Straftat wie etwa Einbruch oder Diebstahl gegen die Gaststätte bekannt geworden ist. Zwar sei 2016 ein Softeis-Automat gestohlen worden, allerdings waren zu der Zeit die Kameras bereits angebracht, einen Beitrag zur Aufklärung des Verbrechens konnten diese aber nicht leisten.

Daraufhin erbat der TLfDI von der Stadt den Namen des Betreibers, um diesen kontaktieren zu können. Nach Erhalt der Auskunft sendete der TLfDI dem Betreiber einen Fragebogen zu, in dem er zu der Videoüberwachung Stellung nehmen konnte. Denn gemäß § 6b Bundesdatenschutzgesetz (BDSG) ist die Beobachtung öffentlich

zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Als Antwort erhielt der TLfDI die Information, dass die Kameras bereits entfernt wurden. Zur Bestätigung sendete der Betreiber Fotografien der Außenwand an der sich die Kameras befunden hatte.

Nach § 6b BDSG ist eine Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.30 Zeugnisverweigerungsrecht schließt Vorgehen des TLfDI nicht aus

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Anzeige eines Anwohners ein, der sich darüber beschwerte, dass an einem Haus in seiner Straße eine Videoüberwachungskamera angebracht worden sei. Der Beschwerdeführer teilte die Adresse sowie den Namen der Person mit, die auf dem Klingelschild an dem Haus aufgeführt war. Zur Sicherheit führte der TLfDI eine Abfrage bei der Meldebehörde der betreffenden Gemeinde durch, um in Erfahrung zu bringen, welche volljährigen Personen unter der genannten Adresse gemeldet waren. Nachdem der TLfDI die Auskunft von der Meldebehörde erhalten hatte, wandte er sich mit einem Auskunftersuchen an den Betreiber. Als keine Reaktion erfolgte, sandte er die gleiche Anfrage nochmals mit Postzustellungsurkunde zu. Daraufhin meldete sich der Rechtsanwalt des Betreibers und forderte zunächst Akteneinsicht, die ihm natürlich gewährt wurde. Der Rechtsanwalt teilte im Anschluss daran mit, dass sich sein Mandant in der Sache nicht erklären werde. Daraufhin erließ der Thüringer Landesbeauftragte ein Auskunftersuchen nach § 38 Abs. 3 Satz 1 i. V. m. Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG). Er wollte wissen, wie viele Videokameras auf dem Grundstück zu welchem Zweck betrieben werden und fragte verschiedene Einzelheiten zum Betrieb der Kameras ab. Hiergegen

legte der Rechtsanwalt des Betreibers Klage beim Verwaltungsgericht Weimar ein. Im Laufe des Verfahrens stellte sich heraus, dass sich der Betreiber auf sein Zeugnisverweigerungsrecht nach § 38 Abs. 3 Satz 2 BDSG beruft. Dies hatte er im vorangegangenen Verwaltungsverfahren nicht deutlich zum Ausdruck gebracht. Der TLfDI nahm daraufhin seinen Bescheid zurück.

Dass der Betreiber einer Videoüberwachungsanlage keine Auskunft über seine Tätigkeit geben muss, sofern er sich damit strafgerichtlicher Verfolgung oder einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde, ändert nichts daran, dass möglicherweise eine unzulässige Videoüberwachungsanlage betrieben wird, gegen die der TLfDI vorgehen muss. Er wandte sich daher an die Stadt mit einem Amtshilfeersuchen und bat um Mitteilung, ob das Gebäude gewerblich genutzt wird und, wie viele Wohneinheiten sich in dem Haus befinden, außerdem um Fotos von der Front des Gebäudes. Die Stadt teilte mit, dass das Gebäude nicht gewerblich genutzt werde. An der Außenwand des Gebäudes waren zwei Kameras befestigt, Hinweise auf die Videoüberwachung fanden sich nicht. Der TLfDI leitete daraufhin ein Ordnungswidrigkeitenverfahren gegen den Betreiber ein und beantragte beim zuständigen Amtsgericht die Beschlagnahme der Videoüberwachungsanlage. Die Polizei vor Ort führte eine Durchsuchung des Gebäudes durch. Die Auswertung des festgestellten Tatbestands ist noch nicht abgeschlossen.

Ein Auskunftspflichtiger kann gegenüber dem TLfDI die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz der Ordnungswidrigkeiten aussetzen würde. Im Rahmen der Durchführung eines Bußgeldverfahrens besteht jedoch die Möglichkeit, nach den Vorschriften der Strafprozessordnung gegen den Betroffenen zu ermitteln. Hierzu gehört auch, dass mit entsprechender amtsgerichtlicher Anordnung eine Hausdurchsuchung, gegebenenfalls mit einer Beschlagnahme, durchgeführt werden kann.

6.31 Videoüberwachung – der TLfDI hilft, wenn er weiß, wo: Videoüberwachung 14

Der Eigentümer eines Mehrfamilienhauses wandte sich mit folgendem Anliegen an den Thüringer Landesbeauftragten für den Daten-

schutz und die Informationsfreiheit (TLfDI): Einer seiner Mieter hatte sich darüber beschwert, dass an dem Autohaus auf dem Nachbargrundstück eine Videoüberwachungsanlage angebracht worden sei. Er forderte die Entfernung der Videokameras, da er diese sogar in seiner Küche auf sich gerichtet sieht. Die Kameras überrückten ebenfalls den öffentlich zugänglichen Innenhof, die gemeinschaftlich genutzten Grünflächen, einige private Stellplätze und die Terrassen der Wohnungen im Erdgeschoss.

Nach § 6b Bundesdatenschutzgesetz (BDSG) ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Die Beobachtungsbefugnis endet an den eigenen Grundstücksgrenzen. In diesem Fall war ein berechtigtes Interesse für die Installation der Kameras nicht ersichtlich. Außerdem wäre eine Alternativlösung wie die Absicherung des Innenhofs durch ein Rollgitter mit Zentralschlüssel möglich gewesen. Auf diese Weise würde weniger in die Persönlichkeitsrechte des Einzelnen eingegriffen.

Der TLfDI wollte die vom Autohaus durchgeführte Videoüberwachung datenschutzrechtlich prüfen, stieß aber auf ein praktisches Problem. Unter der vom Beschwerdeführer genannten Adresse fand sich kein Autohaus und eine Handelsregisteranfrage ergab, dass ein Autohaus mit dem vom Beschwerdeführer genannten Namen nicht existierte.

Der Hauseigentümer wurde daraufhin erneut kontaktiert. Er informierte darüber, dass der sich beschwerende Mieter bereits aus dem Haus ausgezogen ist und der neue Mieter sich durch die Videoanlage nicht gestört fühlt. Der Vermieter sah den Sachverhalt damit als erledigt an und wollte nicht weiter gegen den Gewerbetreibenden vorgehen und war auch nicht bereit, die Adresse des Wohnhauses zu benennen. Da dem TLfDI nur die Adresse des Vermieters, nicht aber die des betroffenen Wohnhauses bekannt war, konnte er die Angelegenheit nicht weiterverfolgen. Gegen den Vermieter konnte der TLfDI nicht vorgehen, da dieser nicht die für die Videoüberwachung zuständige Stelle war.

Der TLfDI kann gegen eine unzulässige Videoüberwachung nur vorgehen, wenn ihm zumindest der Ort des Verstoßes bekannt ist.

6.32 Hotelgäste und Mitarbeiter pausenlos auf Video? Videoga- ga 15

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass die Betreiber eines Hotels unbemerkt für die „Filmstars“ per App das Treiben im Rezeptionsbereich und im Schwimmbad rund um die Uhr in Bild und Ton überwachen könnten.

Da eine „Fernüberwachung“ im Hinblick auf die Datensicherheit problematisch ist, entschied der TLfDI, sich dies nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) vor Ort unangekündigt anzusehen und die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen. Nach § 38 Abs. 4 BDSG ist der TLfDI bzw. sind die von diesem beauftragten Personen zu diesem Zweck befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der zu kontrollierenden Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Diese Personen können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 BDSG sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme einsehen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

Während der unangekündigten Vor-Ort-Kontrolle wurde festgestellt, dass im Bereich der Eingangstheke und im Schwimmbad des Hotels Kameras installiert waren, die Bild und Ton von 22:00 Uhr bis 6:00 Uhr morgens aufnahmen und für sieben Tage auf einer Festplatte eines PCs im Büro des Geschäftsführers speicherten. Eine Abrufbarkeit über eine App auf mobile Endgeräte konnte nicht festgestellt werden. Die Tonaufzeichnung war unverzüglich abzuschalten, da nach § 201 des Strafgesetzbuches sich strafbar macht, wer unbefugt das nicht-öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt. Dem kamen die Betreiber sofort nach. Der TLfDI hat letztendlich keinen Strafantrag gestellt, weil die Prüfung vor Ort ergab, dass zum Zeitpunkt der Kontrolle keine Tonaufnahmen angefertigt wurden und zur Nachtzeit aufgenommene Stimmen nicht verständlich waren und keinen Personen zugeordnet werden konnten. Gegen die Bildaufnahmen zur Wahrung des Hausrechts und zur Sicherheit der Gäste war grundsätzlich nichts einzuwenden, da in jüngster Vergangenheit Einbrüche bzw. unberechtigter Zutritt zum Hotel zu verzeichnen waren. Zur Aufnahmezeit waren die Rezeption

nicht besetzt und das Schwimmbad geschlossen. Also konnte sich im Aufnahmebereich der Kameras eigentlich niemand befugt aufhalten. Auch spät zurückkehrende Hotelgäste mussten diesen Bereich nicht betreten. Allerdings musste die Speicherdauer der Aufnahmen auf der Festplatte des PCs erheblich verkürzt werden, denn für den angegebenen Zweck war nur eine kurze Speicherfrist von maximal 48 Stunden angemessen. In diesem Zeitraum ist es durchaus möglich, etwaige Vorkommnisse festzustellen und auszuwerten.

Da das Hotel aber keinen Datenschutzbeauftragten bestellt hatte, musste es für das Videoüberwachungssystem, auch wenn es letztendlich nur zum Schutz gegen unbefugtes Betreten installiert war, eine Anmeldung gemäß § 4d BDSG zum Register nach § 38 Abs. 2 BDSG beim TLfDI abgeben. Da eine verspätete Meldung zum Register nach § 43 Abs. 1 Nr. 1 BDSG eine Ordnungswidrigkeit darstellt, wird die Einleitung eines Bußgeldverfahrens geprüft.

Videouberwachung zur Wahrung des Hausrechts eines Hotels ist zulässig, wenn dokumentierte Vorkommnisse wie Einbrüche oder unbefugter Zugang zu Nachtzeiten vorliegen. Tonaufnahmen sind immer unzulässig und sogar strafbar. Hat ein Unternehmen keinen eigenen Datenschutzbeauftragten nach § 4f BDSG bestellt, muss es die eingesetzte Videotechnik dem TLfDI zum Register nach § 38 Abs. 2 BDSG melden.

6.33 Grundstücksgrenze = Ende der Beobachtungsbefugnis

Eine Anwohnerin wandte sich an das für sie zuständige Ordnungsamt. Ihr Nachbar hatte an seinem Haus eine Kamera angebracht. Im Erfassungsbereich der Kamera lagen die öffentliche Straße sowie das Grundstück der Beschwerdeführerin. Das Ordnungsamt leitete die Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter. Der TLfDI schrieb daraufhin den Eigentümer des Hauses mit der installierten Videoüberwachungsanlage an und verlangte weitere Informationen bezüglich der installierten Kamera.

Dieser teilte dem TLfDI mit, dass die Kamera noch nicht in Betrieb sei, dies jedoch zeitnah geschehen solle. Der Zweck der Kamera sei die Abschreckung von Straftätern, da es in der Vergangenheit schon mehrfach Vorkommnisse gegeben habe. Unter anderen sei der Briefkasten gesprengt worden. Außerdem befände sich in dem Gebäude

ein Lager mit Waren im Wert von über 150.000 €. Der Eigentümer erläuterte zudem, dass nur das eigene Grundstück überwacht werden solle, öffentlich zugängliche Räume sollen nicht von der Kamera erfasst werden. Die Inbetriebnahme der Kamera solle erst geschehen, wenn deren Zulässigkeit derer durch den TLfDI geprüft wurde.

Der TLfDI kam zu dem Ergebnis, dass, solange die Kamera nur auf das Privatgrundstück und nicht auf den öffentlich zugänglichen Bereich gerichtet ist, keine datenschutzrechtlichen Bedenken bestehen. Eine Meldepflicht nach § 4d BDSG besteht nicht, weil die personenbezogenen Daten nur für eigene Zwecke

erhoben werden, § 4d Abs. 3 Satz 1 BDSG. Sobald die Kamera aber auf Bereiche außerhalb des eigenen Grundstücks gerichtet wird, muss die Videoüberwachungsanlage nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) dem TLfDI gemeldet werden, da in diesem Fall nicht mehr von einer rein persönlichen Nutzung ausgegangen werden kann.



Dies wurde auch durch das Urteil des Verwaltungsgerichts Saarlouis vom 18. Mai 2016 bestätigt (vgl. hierzu die Pressemitteilung des TLfDI vom 19. Mai 2017 unter <https://www.tlfdi.de/mam/tlfdi/presse/pm19052016.pdf>).

Nachdem der TLfDI die Zulässigkeit der angebrachten Kamera festgestellt hatte, teilte er dies dem zuständigen Ordnungsamt und der Beschwerdeführerin mit.

Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig, allerdings endet die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen. Sobald die Kamera auf Bereiche außerhalb des eigenen Grundstücks gerichtet wird, muss die Videoüberwachungsanlage nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) dem TLfDI gemeldet werden.

6.34 Und weg ist die Attrappe: Videogaga 16

Das Ordnungsamt einer Stadt wurde von aufmerksamen Bürgern darüber informiert, dass sich an einem Gebäude eine private Videoanlage befindet. Der Sachverhalt wurde an dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zuständigkeitshalber weitergegeben. Der TLfDI ist nach § 42

Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) und § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) die zuständige Behörde für den Datenschutz. Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Der TLfDI kontaktierte den Eigentümer, bat diesen, den Einsatz seiner Videoüberwachungstechnik darzulegen und konkrete Fragen zur Art und Speicherung der Daten zu beantworten. Der Eigentümer des Gebäudes berichtete, es handle sich schlicht um eine Attrappe einer Überwachungsanlage.

Das vom Bundesverfassungsgericht in seiner Erklärung zur Volkszählung vom 15. Dezember 1983 weiterentwickelte Grundrecht auf informationelle Selbstbestimmung beinhaltet auch einen Schutz gegen Kameraattrappen.

Der TLfDI klärte den Eigentümer auf, dass, wenn eine Attrappe nicht von einer tatsächlich betriebenen Kamera zu unterscheiden ist, davon trotzdem ein Überwachungsdruck ausgeht. Denn das Bundesverfassungsgericht hat in seiner Entscheidung 1 BvR 209/83 u. a. vom 15. Dezember 1983 festgestellt, dass eben wesentlicher Inhalt der informationellen Selbstbestimmung der ist, dass dem Einzelnen bekannt ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Damit liegt ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Dazu bedarf es einer Rechtsgrundlage oder einer Einwilligung. Daraufhin teilte der Eigentümer des Gebäudes mit, dass die Kameraattrappen bereits entfernt worden seien.

Das BDSG beinhaltet auch einen Schutz gegen Kameraattrappen, da für unbeteiligte Dritte trotzdem der Eindruck erweckt wird, aufgenommen zu werden. Datenschutzrechtlich wird daher eine Kameraattrappe durch den TLfDI gleichermaßen gewertet wie eine tatsächlich funktionierende Kamera. Nach § 6b Absatz 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Es ist nicht zulässig, wenn benachbarte Grundstücke oder Straßen im Erfassungsbereich der Kamera liegen.

6.35 Kamera als Abschreckung zulässig?: Videogaga 17

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte Kenntnis darüber, dass in einem Hauseingang im Erdgeschoss eines Mietobjektes eine Überwachungskamera installiert wurde. Die Mieter hatten sich bereits an den Hauseigentümer gewandt, der die Kamera angebracht hatte, jedoch war dieser nicht bereit, die Kamera wieder abzumontieren und erklärte außerdem, dass es sich lediglich um eine Attrappe handle. Dies bestätigte er ebenfalls dem TLfDI auf dessen Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG).

Die Kameraattrappe sei zum Schutz vor illegalen Aktivitäten angebracht worden, da sich in dem Wohnhaus schon mehrfach nicht identifizierbare Personen befunden haben. Der TLfDI klärte den Hauseigentümer über die Voraussetzungen einer zulässigen Videoüberwachung auf. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_durch-nicht-ffentliche-stellen.pdf veröffentlicht ist. Hierauf wurde der Eigentümer hingewiesen. Nach Rücksprache mit seinem Anwalt hat der Vermieter sich daraufhin entschlossen, die Kameras zu entfernen.



Sollten Bewohner eines Mietshauses feststellen, dass dort eine Videoüberwachung vorliegt, können sie sich an den TLfDI wenden. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.36 Videoüberwachung durch Rechtsanwaltskanzlei

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen seiner aufsichtsbehördlichen Tätigkeit darauf aufmerksam gemacht, dass durch eine Rechtsanwaltskanzlei missbräuchlich die Halterdaten eines Beschwerdeführers ermittelt worden sein sollen. Letztendlich wurde seitens des TLfDI festgestellt, dass diese Beschwerde unbegründet war, jedoch wurde im Rahmen dieser Ermittlungen aufgedeckt, dass die angezeigte Kanzlei eine umfangreiche Videoüberwachung auf ihrem Gelände betrieb.

Durch das Beobachten mittels Videokameras werden personenbezogene Daten erhoben und, falls diese Daten auch gespeichert werden, gleichzeitig auch verarbeitet. Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt hat. Deshalb hat der TLfDI die Zulässigkeit der Videoüberwachung anhand der geltenden Gesetze zu prüfen.

Mithilfe eines Auskunftersuchens nach § 38 Abs. 3 BDSG konnte der Sachverhalt ermittelt und so eine Kontrolle der Videoüberwachungsanlage ermöglicht werden. Es waren insgesamt sechs Videokameras auf dem Kanzleigelände installiert, die auf den Eingangsbereich mit Pkw-Stellplätzen, das übrige Grundstück und den Innenhof gerichtet waren. Die Aufnahmen wurden 96 Stunden auf einer Festplatte gespeichert. Ein Hinweisschild befand sich im Eingangsbereich an der Klingel und trug die Aufschrift: „Dieses Objekt wird videoüberwacht“.

Die Zulässigkeit der Videoüberwachung muss hinsichtlich des Zwecks und des Erfassungsbereichs für jede installierte Videokamera einzeln beurteilt werden. Daher sind solche Verfahren, die auch die Vielzahl im aufsichtsbehördlichen Bereich darstellen, in der Regel sehr zeit- und arbeitsaufwendig.

Die Videokameras, die auf den Eingangsbereich sowie auf die Pkw-Stellplätze der Kanzlei gerichtet waren, beurteilen sich nach § 6b BDSG, da es sich bei diesem Bereich um einen öffentlich zugänglichen Raum handelt. Öffentlich zugänglich sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. Grundstückseigentümer) von jedermann genutzt

oder betreten werden dürfen. Während der Öffnungszeiten der Anwaltskanzlei ist davon auszugehen, dass es sich bei dem Eingangsbereich mit den dazugehörigen Pkw-Stellplätzen um einen öffentlich zugänglichen Raum handelt, da dann vorab eine unbestimmte Personengruppe (Mandanten und solche, die es werden wollen sowie anderen Personen) diesen Bereich passiert. Der Bereich des übrigen Grundstücks und des Innenhofs ist als nicht-öffentlicher Raum zu betrachten, da dieser Bereich nicht von jedem, sondern nur von einem bestimmten und abschließend definierten Personenkreis betreten werden kann. Das sind in dem vorliegenden Fall die Eigentümer und Mitglieder der Kanzlei. Insofern wird die Zulässigkeit der Kameras, die auf den Park und Innenhof gerichtet sind, nicht nach § 6b BDSG, sondern nach § 28 Abs. 1 Nr. 2 BDSG beurteilt. Beide unterliegen aber ähnlichen Voraussetzungen.

Eine Videoüberwachung nach § 6b Abs. 1 BDSG ist dann zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Auch im Rahmen des § 28 Abs. 1 Nr. 2 ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung überwiegen. Diese Voraussetzungen konnten seitens der Kanzlei alle erfüllt werden. Der TLfDI bemängelte jedoch das von der verantwortlichen Stelle angebrachte Hinweisschild dahingehend, dass die verantwortliche Stelle mit den entsprechenden Kontaktdaten hierauf nicht zu erkennen war. Der Betroffene muss problemlos, ohne weitere Zwischenschritte, feststellen können, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann.

Darüber hinaus war die Speicherdauer der personenbezogenen Daten zu lang und daher ebenfalls zu bemängeln. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind, § 6b Abs. 5 BDSG. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist und dies festgestellt werden konnte. Ob eine Sicherung notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Deswegen hält der TLfDI

im vorliegenden sowie vergleichbaren Fällen eine Speicherdauer von max. 48 Stunden für erforderlich, aber auch ausreichend. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, etwa wenn an Wochenenden und Feiertagen kein Geschäftsbetrieb erfolgt. Dies ist jedoch seitens der verantwortlichen Stelle vorzutragen. Die Anwaltskanzlei kam sämtlichen seitens des TLfDI gemachten Forderungen nach, sodass die Videoüberwachung nach Einschreiten des TLfDI nunmehr im zulässigen Rahmen betrieben wird.

Grundsätzlich ist zwischen einer Videoüberwachung in öffentlich zugänglichen Räumen und nicht-öffentlich zugänglichen Räumen zu unterscheiden. Diese Unterscheidung bekommt Bedeutung im Rahmen der Hinweispflicht nach § 6b Absatz 2 BDSG. Diese besteht nur für öffentlich zugängliche Bereiche und ist Rechtmäßigkeitsvoraussetzung für die Datenverarbeitung. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen in Form eines entsprechenden Hinweises erkennbar zu machen. Dabei kann der Hinweis mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Der Hinweis ist so anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Er muss in die Lage versetzt werden, der Überwachung ggfs. ausweichen oder sein Verhalten anpassen zu können. Auch die für die Datenverarbeitung verantwortliche Stelle, welche die Videodaten erhebt, verarbeitet oder nutzt, muss mit Adresse angegeben sein. Die Kontaktdaten sind daher auf dem Hinweisschild explizit zu nennen, was viele Kamerabetreiber nicht beachten und was seitens des TLfDI häufig beanstandet werden muss.

6.37 Allgemeine Anfragen zur Videoüberwachung

Während des Berichtszeitraums hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene Anfragen hinsichtlich des Betriebens von Videoüberwachungsanlagen erhalten.

Zum einen wurde von einer niederländischen Datenschutzaufsichtsbehörde angefragt, inwieweit eine Überwachung von Saunaeingängen, insbesondere der angebrachten Drehkreuze, zulässig sei. Besonders war zu berücksichtigen, dass es sich hierbei um eine Sauna mit

homosexuellen Gästen handelte. Die Beurteilung der Zulässigkeit von Videoüberwachungen in einem solchen Bereich richtet sich nach § 6b Bundesdatenschutzgesetz (BDSG). Danach ist eine Videoüberwachung von öffentlich zugänglichen Räumen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Problematisch ist hier insbesondere die Erforderlichkeit für den zumeist verfolgten Zweck, den unbefugten Zutritt von Personen zu verhindern. Die reine Überwachung der Drehkreuze ist in diesem Fall nicht erforderlich, da durch Erhöhen der Drehkreuze der unbefugte Zutritt zu der Sauna oder auch zu Schwimmbädern erschwert werden kann. Darüber hinaus kann die Sexualität der Besucher nach § 3 Abs. 9 BDSG eine besondere Art von personenbezogenen Daten sein, was im Rahmen der Abwägung der schutzwürdigen Interessen mit den berechtigten Interessen des Kamerabetreibers zu berücksichtigen ist und auch zum Überwiegen der Interessen der Betroffenen führen kann. Eine generelle Unzulässigkeit kann hieraus jedoch nicht hergeleitet werden.

Eine weitere Anfrage kam von einem Bürger, welcher wissen wollte, an wen man sich wendet, wenn eine private Videoüberwachung den öffentlichen Raum miterfasst und wie man diese abstellen kann. Zwar kann ein privater Hauseigentümer im Rahmen seines Hausrechts grds. sein eigenes Grundstück überwachen. Eine solche Überwachung fällt unter die Privilegierung des § 1 Abs. 2 Nr. 3 BDSG, da die personenbezogenen Daten lediglich zu familiären und persönlichen Zwecken erhoben, verarbeitet oder genutzt werden. In einem solchen Fall sind die Vorschriften des BDSG nicht anwendbar. Geht die Überwachung jedoch über die eigenen Grundstücksbereiche hinaus, werden also Straßen, Gehwege oder Nachbargrundstücke erfasst, also außerhalb der privaten Sphäre desjenigen, der Daten auf diese Weise verarbeitet, kann sie nicht als eine ausschließlich „persönliche oder familiäre“ Tätigkeit angesehen werden. Das hat der Europäische Gerichtshof in seinem Rynes-Urteil vom 11. Dezember 2014 Az.: C-212/13 abschließend entschieden. In einem solchen Fall können sich Betroffene an die örtlich zuständige Aufsichtsbehörde für den Datenschutz wenden. Für Thüringen ist dies der TLfDI. Die Aufsichtsbehörde prüft dann die Vereinbarkeit der Videoüberwachungsanlage mit den Vorschriften des BDSG. Sollte ein Verstoß vorliegen, wird die Aufsichtsbehörde entspre-

chende Anordnungen treffen und diese durchsetzen. Ferner ist es möglich, den Zivilrechtsweg einzuschlagen und gegen die Persönlichkeitsrechtsverletzung, welche durch eine Videokamera hervorgerufen wird, vorzugehen.

Der Einsatz von Videoüberwachungen kommt in allen Bereichen des täglichen Lebens vor. Jede Entscheidung über die Zulässigkeit der eingesetzten Videoüberwachung ist eine Einzelfallbetrachtung, deswegen können solche allgemeinen Fragen nur oberflächlich beantwortet und insgesamt nur generelle Aussagen getroffen werden. Verantwortlich für diese Zulässigkeitsprüfung ist jedoch der Verwender der Videoüberwachung, und zwar bevor diese eingerichtet wird. Nach Erfahrung des TLfDI ist Videoüberwachung nämlich in

der Regel zumindest in Teilen unzulässig, wenn diese geprüft wird. Der TLfDI stellt den nicht-öffentlichen Stellen auf seiner Website die „Orientierungshilfe Videoüberwachung durch nicht-öffentlichen Stellen“ (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf) als Hilfe und Information zur Verfügung.



Zusätzlich weist der TLfDI darauf hin, dass alle Videoüberwachungen von nicht-öffentlichen Stellen nach § 4d Abs. 1 BDSG zu melden sind, soweit die Ausnahmetatbestände des § 4d Abs. 2 und 3 BDSG nicht eingreifen. Die entsprechenden Meldeformulare mit Anlage sind ebenfalls auf der Website des TLfDI abrufbar

(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v_.pdf,

https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_v_anlagenformular.pdf).



Der Einsatz von Videoüberwachungen ist vielfältig und kommt mittlerweile in fast sämtlichen Lebensbereichen vor. Die Anfragen und Beschwerden beim TLfDI nehmen daher immer mehr zu. Diese sind genauso vielseitig wie die Einsatzbereiche der einzelnen Videoüberwachungskameras selbst.

6.38 Videoüberwachungsverbesserungsgesetz – Verbesserung? – Anwendbarkeit?

Das am 4. Mai 2017 in Kraft getretene „Videoüberwachungsverbesserungsgesetz“ – Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen - musste bereits im Vorfeld seiner Verabschiedung erhebliche Kritik der Datenschutzbehörden von Bund und Ländern einstecken. Das Gesetz sieht in § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) (neu) vor, dass bei einer Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren, Parkplätzen oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse gilt. Die Gesetzesänderung soll dazu beitragen den privaten Stellen das Betreiben der Videoüberwachung zu erleichtern. Vordergründig sollen mit dem Gesetz insbesondere terroristische Anschläge wie in Ansbach, Berlin oder München durch die Ausweitung der Videoüberwachung privater Stellen verhindert und die Sicherheit der Bevölkerung erhöht werden.

Die einzelnen Datenschutzbehörden der Länder waren sich darin einig, dass solche Anschläge mittels Betreibens einer Videoüberwachung nicht verhindert werden können. Hierzu wäre eine Videoüberwachung auf den in dem Gesetz genannten Plätzen erforderlich, die eine Live-Beobachtung ermöglicht. Außerdem müsste das gleichzeitige Eingreifen eines Wachschutz- oder Sicherheitspersonals bei einem Vorfall gegeben sein. Das ist bei den Videoüberwachungsanlagen meist nicht der Fall, da die hohen Kosten für zusätzliches Personal die Unternehmen abschrecken. Meist kommen hier sog. Black-Box-Verfahren zum Einsatz. Die personenbezogenen Daten werden gespeichert und für eine gewisse Dauer zum Abruf

bereitgehalten. Hierdurch wird lediglich im Nachgang die Möglichkeit der Strafverfolgung durch die zuständigen Behörden erleichtert. Eine tatsächliche Erhöhung der Sicherheit der Bevölkerung geht damit nicht einher. Lediglich das subjektive Sicherheitsgefühl der Personen wird hierdurch gesteigert. In der Praxis sind die Betreiber zumeist nicht in der Lage, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. Zudem verkennt der Referentenentwurf des Bundesinnenministeriums zu dem Gesetz, dass Terroristen und irrational handelnde Einzeltäter ihren eigenen und den Tod der anderen bewusst in Kauf nehmen und gerade die öffentliche Zurschaustellung ihrer Taten beabsichtigen.

Darüber hinaus wurden bereits im Rahmen der alten Regelung des § 6b Abs. 1 BDSG die Sicherheitsinteressen von Unternehmen hinsichtlich des Zwecks Hausrecht und berechnete Interessen sowie der Schutz von Leib und Leben im Rahmen der Abwägung der schutzwürdigen Interessen von den Datenschutzbehörden hinreichend berücksichtigt, sofern der private Betreiber eine tatsächliche Gefahrenlage für diese Rechtsgüter nachweisen konnte. Ein Überwiegen dieser Interessen gegenüber dem informationellen Selbstbestimmungsrecht der Betroffenen lag dann i. d. R. auch vor. Jedoch kam dies immer auf den Einzelfall an, da jede Videoüberwachung einer Einzelfallprüfung unterliegt. Letztendlich ist die Regelung darauf gerichtet, dass dem Schutz von Leib und Leben in der rechtlichen Abwägung ein stärkeres Gewicht zuzumessen ist, was aber auch der bisherigen aufsichtsbehördlichen Praxis entspricht. Eine abstrakte Gefährdung aller großflächigen Anlagen und des Personennahverkehrs hinsichtlich der im Gesetz genannten Rechtsgüter wird durch die Aufsichtsbehörden der Länder bezweifelt.

Abschließend ist noch darauf hinzuweisen, dass sich die Aufsichtsbehörden der Länder darin einig sind und waren, dass es nicht Aufgabe der privaten Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Diese Aufgabe obliegt nicht ohne Grund den Sicherheitsbehörden des Bundes und der Länder. Die Gesetzesänderung stellt aber gerade eine solche Übertragung der hoheitlichen Aufgabe Schutz und Sicherheit der Bevölkerung auf Private dar.

Trotz dieser Bedenken und Einreichung einer umfangreichen Stellungnahme durch die Datenschutzkonferenz aller Datenschutzbehörden von Bund und Ländern wurde die Gesetzesänderung beschlossen

und in Kraft gesetzt. Wie sich diese Änderung bei der Beurteilung der Zulässigkeit der zu prüfenden Videoüberwachungsanlagen auswirken wird, ist noch nicht absehbar. Ab dem 25. Mai 2018 wird außerdem die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) Geltung in allen europäischen Staaten der EU erlangen. Der Bundesgesetzgeber hat in einem seit dem 5. Juli 2017 in Kraft getretenem Anpassungsgesetz zu dieser Verordnung (EU-DSAnpUG-EU) mit § 4 EU-DSAnpUG EU eine eigene Regelung hinsichtlich des Betriebes von Videoüberwachungskameras in öffentlichen Bereichen von privaten Stellen getroffen, welche dem jetzt geänderten § 6b Abs. 1 BDSG entspricht. Auch hier ist noch unklar, ob diese Regelung überhaupt seitens der Aufsichtsbehörden bei der Zulässigkeitsprüfung angewendet werden kann, da das europäische Recht den nationalen Gesetzen vorgeht und die Europäische Datenschutz-Grundverordnung dem nationalen Gesetzgeber keine Befugnis zu eigenen Regelungen in diesem Bereich eingeräumt hat.

Am 4. Mai 2017 ist das „Videoüberwachungsverbesserungsgesetz“ – Gesetz zur Änderung des Bundesdatenschutzgesetzes – zur Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen – in Kraft getreten. Es regelt, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in den im Gesetz genannten Anlagen aufhalten, als besonders wichtiges Interesse gilt. Ziel der Gesetzesänderung ist es, dass durch Ausweitung der Videoüberwachung der privaten Stellen eine höhere Sicherheit der Bevölkerung erreicht werden soll. Bereits im Gesetzgebungsverfahren wurde die Gesetzesänderung von den Aufsichtsbehörden abgelehnt. Trotz der Bedenken ist das Gesetz in Kraft getreten. Inwieweit sich in der Praxis hierdurch Änderungen hinsichtlich der Beurteilung der Zulässigkeit von Videoüberwachungen ergeben, ist noch nicht absehbar. Eine abstrakte Gefährdung aller großflächigen Anlagen und des Personennahverkehrs hinsichtlich der im Gesetz genannten Rechtsgüter wird durch die Aufsichtsbehörden des Bundes und der Länder insoweit nicht angenommen, sodass weiterhin Einzelfallprüfungen erfolgen. Ob das neue Recht angesichts der Anwendungsvorrang genießenden EU-DS-GVO überhaupt anzuwenden ist, wird gerade diskutiert.

6.39 Keine Meldepflicht bei Firmenüberwachung?

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) durch eine Firma angefragt, ob eine Videoüberwachung auf dem Firmengelände meldepflichtig sei, wenn keine festangestellten Mitarbeiter dort beschäftigt sind und nur zeitweise ein Geschäftsbetrieb erfolgen würde. Hierzu teilte der TLfDI dem betreffenden Firmeninhaber mit, dass auch diese Videoüberwachung zu melden sei. Nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) sind Verfahren automatisierter Verarbeitungen vor der Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe der Angaben aus § 4e BDSG zu melden. Digitale Videoüberwachungen stellen grundsätzlich ein meldepflichtiges Verfahren dar, da es sich dabei immer auch um eine automatisierte Verarbeitung handelt. Hierbei ist nicht relevant, ob das Firmengelände nur zeitweise genutzt wird oder keine festangestellten Mitarbeiter dort tätig sind, da jedenfalls zu den Zeiten, in denen sich Personen auf dem Gelände aufhalten, personenbezogene Daten automatisiert verarbeitet werden. Eine Unterscheidung zwischen Personen, die fest angestellt sind, und solchen, die nur vorübergehend beschäftigt sind, nimmt das BDSG – glücklicherweise – nicht vor.

Die Meldepflicht entfällt allerdings dann, wenn seitens der verantwortlichen Stelle ein Beauftragter für den Datenschutz bestellt wurde, § 4d Abs. 2 BDSG. Ein weiterer Ausnahmetatbestand liegt vor, wenn die Daten für eigene Zwecke erhoben, verarbeitet oder genutzt werden, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind und eine Einwilligung des Betroffenen vorliegt (§ 4d Abs. 3 BDSG). Beide Ausnahmetatbestände wurden durch die anfragende Firma nicht vorgetragen, sodass die von ihr geplante Videoüberwachung zu melden war.

Digitale Videoüberwachungen von nicht-öffentlichen Stellen unterfallen generell der Meldepflicht nach § 4d Abs. 1 BDSG, sofern die vorhergehend genannten Ausnahmetatbestände nicht eingreifen. Durch die Entscheidung des Verwaltungsgerichts Saarland vom 18. Mai 2016 Az. 1 K 63/15 wurde diese generelle Meldepflicht nunmehr bestätigt. Der TLfDI stellt auf seiner Website den Unternehmen entsprechende Meldeunterlagen bereit, um den verantwortli-

chen Stellen eine Meldung in das durch den Landesbeauftragten für den Datenschutz zu führende Melderegister nach § 38 Abs. 2 BDSG zu erleichtern und einen Leitfaden an die Hand zu geben. Diese Meldeunterlagen sind auf der Website unter <https://www.tlfdi.de/tlfdi/datenschutz/videoueberwachung.de> abrufbar.



6.40 Baden und Entspannen unter Beobachtung – Videogaga 18

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen einer Umfrage einer anderen Aufsichtsbehörde um Mitteilung gebeten, inwieweit eine Beurteilung der Zulässigkeit der Videoüberwachung eines bestimmten Spaßbades erfolgt ist. Da ein solches Spaßbad keinen Standort in Thüringen hatte, konnte kein Kontakt festgestellt oder eine Bewertung vorgenommen werden. Kontakte zu Schwimmbädern in Thüringen hatte und hat der TLfDI jedoch in diesem Zusammenhang bereits mehrfach.

Die Videoüberwachung in Schwimmbädern oder Spaßbädern beurteilt sich nach dem Bereich, in dem sie eingesetzt werden soll und dem hierfür festgelegten Zweck unterschiedlich. Insbesondere genießen Schwimmbadbesucher besonderen Schutz, da sie sich im Schwimmbad/Erlebnisbad zum Zweck der Freizeitgestaltung aufhalten und eine Videoüberwachung in diesem Bereich einen sehr intensiven Eingriff in deren informationelles Selbstbestimmungsrecht darstellt. Zum Einsatz von Videoüberwachungen in Schwimmbädern wurde im Rahmen des Düsseldorfer Kreises eine Orientierungshilfe erarbeitet, welche der TLfDI auf seiner Website https://www.tlfdi.de/mam/tlfdi/datenschutz/video/01_zusatz_zur_oh_v_.pdf zur Verfü-



gung stellt. Dort werden die wichtigsten Fakten zur Zulässigkeit von Videoüberwachungen in Schwimmbädern aufgeführt. Die Zulässigkeit der Videoüberwachung beurteilt sich, wenn es sich um Schwimmbäder in privater Trägerschaft handelt, während der Öffnungszeiten nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Das Beobachten mit Videokameras ist danach nur dann zulässig, soweit dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Auch hier ist immer eine **Einzelfallprüfung** vorzunehmen. Jedoch kann man folgende allgemeine Hinweise geben:

Im Eingangs- und Kassenbereich eingesetzte Videoüberwachung zur Verhinderung des unbefugten Zutritts oder von Manipulationen oder Beschädigungen von Kassenautomaten wird zumeist nicht erforderlich sein. An der Erforderlichkeit fehlt es, wenn der Zweck auch mit anderen, weniger einschneidenden Mitteln erreicht werden kann, z. B. hier durch Positionierung von Kassenautomaten im Sichtfeld des Kassenpersonals oder Erhöhen der Drehkreuze.

Die Überwachung von Umkleidekabinen, Duschen, Saunen und Toilettenräumen als geschützte Bereiche der Intimsphäre stellt einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Badegäste dar. Eine Videoüberwachung ist dort **immer** unzulässig.

Differenziert sind die Kleider- und Wertspindschließfächer zu betrachten. Sofern eine Trennung von Umkleidekabine und Wertschließfach vorliegt, ist es möglich, den Bereich zu überwachen, jedoch ist darauf zu achten, dass die spärlich bekleideten Badebesucher nicht in den überwachten Bereich gelangen, d. h., die Kameras sind entweder nur auf den Spind zu richten oder den Badegästen ist eine Wahlmöglichkeit zu lassen, indem man Bereiche, die nicht überwacht werden, kennzeichnet. Problematisch wird die Videoüberwachung in jedem Fall dann, wenn die Spindbereiche mit Bänken oder anderen Sitzmöglichkeiten ausgestattet sind. Dann sind diese als Umkleidebereich zu werten, was zur Unzulässigkeit der Videoüberwachung führt.

Die personenscharfe Überwachung des Bade- und Ruhebereichs ist im Regelfall unzulässig. Sofern es nur um die Feststellung von Verstößen gegen die Haus- und Badeordnung geht, stehen die schutzwürdigen Interessen der Badebesucher entgegen. Ein Ausschluss des

Haftungsrisikos gegenüber Ansprüchen von Badegästen ist ebenfalls wegen des Überwiegens schutzwürdiger Interessen von Betroffenen unzulässig. Zudem unterliegt eine mögliche Haftung der Beweis-pflicht des Geschädigten.

Im Badebereich kann eine Videoüberwachung jedoch zur Unterstützung der Aufsicht in besonders gefahrträchtigen Bereichen (z. B. Sprungtürme, Rutschen, Kinderbecken) in Betracht kommen. Die Gefährlichkeit muss sich aufgrund objektiver Anhaltspunkte ergeben. Der Einsatz der Videoüberwachung kann aber kein Ersatz für die Aufsicht durch das Badepersonal sein, deswegen sind eine Speicherung und eine personenscharfe Videoüberwachung nicht erforderlich. Ein Monitoring ohne personenscharfe Aufnahmen ist hier ausreichend, sofern die Möglichkeit besteht, dass das Badepersonal die Kamerabilder ständig überwacht, um im Notfall schnell eingreifen zu können. Zudem ist darauf hinzuweisen, dass eine reine Aufzeichnung (sog. Black-Box-Verfahren) für rein präventive Zwecke nicht geeignet ist, da dann keine Interventionsmöglichkeit besteht. Das bedeutet, dass eine solche Videoaufzeichnung zur Verhinderung von Unfällen oder gar Straftaten nicht geeignet und damit nicht erforderlich ist.

Die Schwimmbadbetreiber sollten sich generell vor dem Einsatz einer Videoüberwachungsanlage hinsichtlich des Zwecks und auch des Einsatzes von möglichen mildereren Mitteln genaue Gedanken machen und ggfs. zuvor den TLfDI um Rat fragen.



Zum Einsatz von Videoüberwachungen in Schwimmbädern wurde im Rahmen des Düsseldorfer Kreises eine Orientierungshilfe erarbeitet, welche der TLfDI auf seiner Website https://www.tlfdi.de/mam/tlfdi/datenschutz/video/01_zusatz_zur_oh_v_.pdf zur Verfügung stellt. Dort werden die wichtigsten Fakten zur Zulässigkeit von Videoüberwachungen in Schwimmbädern aufgeführt. Aufgrund der ab Mai 2018 Geltung erlangenden Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) und des seit

Anfang Juli in Kraft getretenen Anpassungsgesetzes zur EU-DS-GVO können sich hierzu Änderungen ergeben. Alle Orientierungshilfen hinsichtlich von Videoüberwachungen im nicht-öffentlichen Bereich werden entsprechend der neuen Gesetze überarbeitet.

6.41 Videoüberwachung im Restaurant – bei nebulösen Angaben keine Beratung

Während seiner aufsichtsbehördlichen Tätigkeit bekam der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seitens einer Rechtsanwaltskanzlei eine Beratungsanfrage zu einer Videoüberwachung in einem Restaurantbetrieb. Die Anwaltskanzlei übersandte lediglich eine Skizze, auf der die geplanten Videokameras eingezeichnet waren, sonstige Angaben erfolgten nicht. Grundsätzlich hat die Aufsichtsbehörde nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) die verantwortlichen Stellen sowie die Beauftragten für den Datenschutz auf deren typische Bedürfnisse hin zu beraten. Jedoch ist dabei zu berücksichtigen, dass ein entsprechendes datenschutzrechtliches Konzept vorgelegt werden sollte, damit der TLfDI eine Bewertung zur Zulässigkeit machen kann. Die Zulässigkeit von Videoüberwachungsanlagen beurteilt sich entweder nach § 6b BDSG für öffentlich zugängliche Bereiche oder nach § 28 Abs. 1 Nr. 2 BDSG für den nicht-öffentlich zugänglichen Bereich. Auf Grundlage dieser beiden Erlaubnisnormen ist ein Konzept seitens der verantwortlichen Stellen zu entwickeln. Insbesondere ist zu erarbeiten, welche Zwecke mit der Videoüberwachung verfolgt werden sollen. Darüber hinaus ist bei der Zulässigkeitsprüfung die Erforderlichkeit der Videoüberwachung für diese Zwecke zu erörtern. Insbesondere ist dabei darzustellen, ob es für den genannten Zweck nicht ein anderes gleich geeigneteres Mittel gibt. Die verantwortlichen Stellen sollten sich hier Gedanken über mögliche Alternativen zu der Videoüberwachung machen und Gründe benennen können, warum diese Alternativen nicht ergriffen wurden. Weiterhin muss dargelegt werden, wie ein Eingriff in schutzwürdige Interessen vermieden werden kann oder warum die eigenen Interessen am Betreiben der Videoüberwachung überwiegen. Ferner werden technische Angaben der Videoüberwachungsanlage bzw. jeder einzelnen Kamera benötigt, u. a. Marke/Typenbezeichnung der Kamera, Schwenk- und Zoomfähigkeit, Audiofunktion, Auflösung (bestmögliche), Sichtwinkel, Beobachtung (Monitoring) oder Aufzeichnung

sowie Dauer der Speicherung, Löschung der Daten, Personenabgleich/Gesichtserkennung. Zusätzlich zu den technischen Angaben der Kameras sind schriftliche Festlegungen in Form von technisch-organisatorischen Maßnahmen gem. § 9 Satz 1 BDSG zu treffen, um die datenschutzgerechte und sichere Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zu erreichen. Hier können insbesondere Speicherfristen, Betriebszeiten, Zugriffsschutz, Zugangskontrollen etc. festgelegt werden. Diese Angaben wurden allesamt seitens des Mandanten der Rechtsanwaltskanzlei nach Anforderung nicht gemacht, sodass eine abschließende Beratung nicht erfolgen konnte.

Die verantwortlichen Stellen sollten bei einer gewünschten Beratung im Rahmen einer Videoüberwachung durch den TLfDI ein den vorgenannten Angaben entsprechendes datenschutzrechtliches Konzept vorlegen. Hilfreich können hierzu das auf der Homepage des TLfDI hinterlegte Erfassungsblatt für Kameras (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/video_berwachu ng_erfassungsblatt_kameras.pdf) sowie die Orientierungshilfe des Düsseldorfer Kreises (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf) sein. In diesem Zusammenhang wird darauf hingewiesen, dass am 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (DS-GVO) Geltung in allen Mitgliedstaaten der Europäischen Union erlangen wird. Auch aufgrund des zwischenzeitlich am 5. Juli 2017 in Kraft getretenen Anpassungsgesetzes zur EU-DS-GVO werden sich Änderungen hinsichtlich der rechtlichen Grundlagen, aufgrund derer eine Videoüberwachung in Deutschland durchgeführt werden kann, ergeben. Die bis jetzt geltenden Grundsätze in der Orientierungshilfe des Düsseldorfer Kreises für den nicht-öffentlichen Bereich werden insofern an die neue Rechtslage angepasst und überarbeitet.



6.42 Datenschutz: durchgesetzt! – Videogaga 19

Ein weiterer Fall in Sachen Videoüberwachung beschäftigt den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) immer noch. Bereits im 2. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich unter Punkt 4.61 wurde darüber berichtet, dass ein Betreiber einer Videoüberwachungsanlage nicht einsichtig war, dass auch für ihn die gesetzlichen Bestimmungen gelten. Er verweigerte die Beantwortung des Fragenkatalogs vom TLfDI, da es sich um ausgemusterte Vorführgeräte handle und er demzufolge die Fragen nicht beantworten würde. Der Betreiber sollte unter anderem Auskunft darüber geben, auf welche Bereiche die Kameras ausgerichtet sind und er sollte die Ausrichtung mittels eines Lageplans darstellen. Auch wenn es sich um Kameraattrappen handeln sollte, ist der Betreiber gesetzlich verpflichtet, dem Auskunftersuchen des TLfDI nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) nachzukommen und es nicht einfach zu verweigern. Zum Abschluss des Verwaltungsverfahrens ist es bis jetzt noch nicht gekommen.

Wie auch im vorherigen Tätigkeitsbericht schon deutlich zum Ausdruck gebracht, hat der TLfDI als zuständige Aufsichtsbehörde das Mittel der Anordnung unter Androhung eines Zwangsgeldes, um Auskünfte zu erhalten. Denn nur wenn der Sachverhalt feststeht, können rechtliche Bewertungen vorgenommen werden. Zum Mittel des Auskunftsbeseides wird allerdings nur gegriffen, wenn vorher auf einfache Schreiben hin keine Auskunft erteilt wird.

6.43 Wenn der Datenschutz zweimal klingelt

Im 2. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich wurde unter dem Punkt 4.62 über eine installierte Videoüberwachungsanlage eines Hausbesitzers berichtet. Die Videoüberwachungskamera war am Balkon des Hauses angebracht. Wie der Betreiber auf Nachfrage mitteilte, sei lediglich eine Kameraattrappe installiert und er sähe darin keinen datenschutzrechtlichen Verstoß nach dem Bundesdatenschutzgesetz (BDSG). Der Betreiber teilte jedoch dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass die Attrappe abgebaut wurde.

Leider war die Sache damit beim TLfDI nicht abgehakt. Um sicher zugehen, dass die Auskunft des Betreibers auch stimmte, bat der TLfDI die zuständige Stadtverwaltung um Amtshilfe mittels einer Vor-Ort-Kontrolle. Diese stellte dabei fest, dass zwar die Kameraaattrappe am Balkon abgebaut wurde, sich jedoch eine weitere Videoüberwachungskamera auf dem Grundstück befand. Der Hausbesitzer filmte nun von seinem Carport aus Teile seines Hofgrundstücks und die Einfahrt.

Daraufhin wandte sich der TLfDI erneut an den Betreiber, um zu klären, ob die Kamera datenschutzkonform nach § 6b BDSG betrieben wird. Hierbei kommt es insbesondere auf die Ausrichtung der Kamera an und darauf, welche Bereiche sie abbildet. Wenn die Kamera das eigene Grundstück erfasst und öffentlich zugängliche Räume nicht erfasst werden oder durch die Videoüberwachung nicht auf eine andere Weise die persönliche Sphäre verlassen wird, wie dies zum Beispiel durch Erfassen eines Nachbargrundstücks der Fall wäre, ist der Anwendungsbereich des BDSG gemäß § 1 Abs. 2 Nr. 3 schon nicht eröffnet. Der Betreiber bestätigte gegenüber dem TLfDI, dass durch die Kamera keine öffentlich zugänglichen Bereiche des Grundstücks erfasst, also keine Personen gefilmt werden, die auf sein Grundstück gehen müssen, um an der Haustür zu klingeln, an die Haustür zu gelangen und an den Briefkasten zu kommen. Somit konnte in diesem Fall festgestellt werden, dass eine unzulässige Erhebung von personenbezogenen Daten ausgeschlossen ist und der Betreiber konnte die Videoüberwachungsanlage weiter für seine privaten Zwecke nutzen.

Datenschutzrelevant ist der Erfassungsbereich der Kamera auf dem Grundstück. Hier muss unterschieden werden, ob es sich beim Aufnahmebereich um einen öffentlich zugänglichen Bereich handelt oder nicht. Sollte die Videoüberwachung den nicht-öffentlich zugänglichen Bereich erfassen, dann sind die Regelungen im BDSG nur maßgebend, sobald auch das Nachbargrundstück oder fremde Personen aufgenommen werden. Das BDSG greift nicht, wenn nur das eigene Grundstück gefilmt wird. Allerdings ist für den öffentlich zugänglichen Bereich (z. B. der Hauseingang) § 6b BDSG einschlägig.

6.44 Videoüberwachung versus Vandalen

Was wäre der Datenschutz ohne den aufmerksamen Bürger? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhält regelmäßig von Bürgern den Hinweis auf Videoüberwachungsanlagen. Auch im folgenden Fall entdeckte ein Bürger drei Videokameras an einer Garage in Erfurt. Er informierte zunächst die Erfurter Stadtverwaltung. Die Mitarbeiter der Stadtverwaltung reagierten sofort und leiteten die Beschwerde zuständigkeitshalber an den TLfDI weiter.

Der TLfDI wandte sich im Zuge eines Auskunftsverlangens nach § 38 Abs. 3 BDSG an den Nutzer der Garage. Der Besitzer der Garage und somit auch Betreiber der Videokameras wurde aufgefordert, Auskunft über die Videoüberwachungsanlage zu geben, unter anderem, welche Bereiche gefilmt werden und zu welchem Zweck die Videoüberwachung dient. In seiner Antwort begründete der Betreiber, dass er des Öfteren Opfer von Vandalismus auf seinem Grundstück gewesen sei und dies auch mehrfach zur Anzeige bei der Polizei gebracht hätte. Außerdem führte er aus, dass er mit den Videokameras lediglich die „Vandalen“ abschrecken möchte. Seine Kameras waren so ausgerichtet, dass Bereiche vor der Garage gefilmt wurden; über weitere Funktionen wie Zoom- oder Schwenktechnik verfügen die Kameras nicht. Die Nachbargrundstücke waren über feste Filter ausgeblendet. Mit Hinweisschildern an der Garage wurde auf die Videokameras hingewiesen.

Bei einer Videoüberwachung werden aufgrund der Beobachtung personenbezogene Daten erhoben und – sofern die Aufnahmen aufgezeichnet werden – gleichzeitig verarbeitet. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Es verbleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die die Videoüberwachung erlaubt. Einschlägige Rechtsvorschrift bei der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen ist § 6b BDSG. Hierzu ist im § 6b Abs. 1 Nr. 1 bis 3 BDSG klar definiert, unter welchen Voraussetzungen Videoüberwachung bei der Beobachtung von öffentlich zugänglichen Räumen

zulässig ist. So ist nach § 6b Abs. 1 Nr. 1 BDSG Videoüberwachung nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen erforderlich ist, nach § 6b Abs. 1 Nr. 2 BDSG zur Wahrung des Hausrechts und nach § 6b Abs. 1 Nr. 3 BDSG zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke. Bei allen drei Varianten muss die Videoüberwachung erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass das schutzwürdige Interesse der Betroffenen überwiegt.

Eine Überwachung öffentlich zugänglicher Räume liegt z. B. vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden können. Durch die Videoüberwachungsanlage wurde öffentlich zugänglicher Raum im Sinne des § 6b BDSG miterfasst. Nach § 6b Abs. 1 Nr. 2 BDSG beinhaltet das Hausrecht die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann zum einen präventive Zwecke verfolgen, indem Personen davon abgehalten werden sollen, Rechtsverstöße – z. B. Sachbeschädigungen durch Graffiti und Beschädigungen an Garagentüren innerhalb des vom Hausrecht umfassten Bereichs – zu begehen (Störerabwehr), vgl. Scholz, in: Simitis, BDSG, § 6b Rn. 75, 8. Auflage. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtinhabers nur bis an die Grenzen des Grundstücks und nach der Rechtsprechung einen Meter darüber hinaus, vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02. Die dargelegten Gründe zur Wahrung des Hausrechts können ein berechtigtes Interesse des Betreibers der Videoüberwachungsanlage sein, demgegenüber stehen jedoch die schutzwürdigen Interessen der Betroffenen. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort auf-

haltenden Personen mit überwacht werden. Aus den vorgelegten Aufnahmen ergab sich, dass der angrenzende Gehweg zur Garagenfassade lediglich einen Meter betrug und weitere Grundstücke gefiltert/geschwärzt wurden. Der Betreiber der Videoüberwachungskameras stützte sich auf sein Hausrecht. Da sich der Kameraaufnahmebereich innerhalb des einen Meters an der Garagenfassade erstreckte und ausreichend Raum zum Ausweichen gegeben war sowie die angrenzenden Grundstücke gefiltert bzw. geschwärzt waren, beurteilte der TLfDI die Videoüberwachungsanlage zur Wahrung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG als zulässig. Das Verwaltungsverfahren wurde daher als erledigt angesehen.

In Thüringen tauchen vermehrt im privaten Bereich Videoüberwachungskameras auf. Dabei gelten auch für den privaten Bereich die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren .

6.45 Insolvenz schützt nicht vor Datenschutz – Videogaga 20

Aufgrund seiner Kontrolltätigkeit wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass an zwei Wohnblöcken in Ostthüringen eine Videoüberwachung mit jeweils drei Videokameras betrieben wurde. Die Kameras waren auf den Eingangsbereich der Wohngebäude und teilweise auf den öffentlichen Gehweg sowie Straßenbereich gerichtet. Die Eigentümerin wurde mittels Auskunftersuchen des TLfDI angeschrieben, da diese u. U. verantwortliche Stelle gem. § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) ist. Das Schreiben kam jedoch als Postrückläufer zurück. Die weiteren Ermittlungen ergaben, dass die Eigentümerin insolvent war. Der für das Vermögen der Eigentümerin bestellte Insolvenzverwalter wurde seitens des TLfDI angeschrieben und um Mitteilung gebeten, ob das Insolvenzverfahren zwischenzeitlich beendet wurde und wer nun Eigentümer der Gebäude ist. Der Insolvenzverwalter teilte sodann mit, dass das Verfahren immer noch andauere. Daraufhin wandte sich der TLfDI mit dem Auskunftersuchen an den Insolvenzverwalter, da nach § 80 Abs. 1 Insolvenzordnung (InsO) das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten, auf den Insolvenzverwalter übergeht. Insofern tritt der Insolvenzverwalter an die Stelle

der Eigentümerin der Gebäude. Das Verfahren dauert beim TLfDI noch an.

Verantwortliche Stelle ist nach § 3 Abs. 7 BDSG jede verantwortliche Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im vorliegenden Fall trat an die Stelle der bisherigen Eigentümerin aufgrund des eröffneten Insolvenzverfahrens deren Insolvenzverwalter. Nach § 80 Abs. 1 InsO geht das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten, auf den bestellten Insolvenzverwalter über. Der Betrieb der Videoüberwachungsanlage gehört zur Verwaltung des Eigentums, sodass der Insolvenzverwalter als verantwortliche Stelle i. S. d. BDSG zu betrachten ist.

6.46 Hinweis auf Videoüberwachung, aber wo ist die Kamera?

Aufgrund der Mitteilung einer Polizeiinspektion wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass an einer Bushaltestelle sowie an einem dort befindlichen Gebäude Hinweisschilder einer dort vermeintlich betriebenen Videoüberwachung angebracht wurden. Videokameras konnten aber auch nach Inaugenscheinnahme durch die Polizei weder im Bereich der Bushaltestelle noch an dem dahinter befindlichen Grundstück festgestellt werden. Der TLfDI wandte sich daher zunächst mit einem Auskunftsverlangen an die mögliche verantwortliche Stelle der Videoüberwachung, den Eigentümer des Grundstücks. Dieser teilte dem TLfDI mit, dass sich auf dem Grundstück und an der Bushaltestelle keine Kameras befinden würden. Und er könne Schilder anbringen wie er wolle. Da die Polizei keine Videokameras feststellen konnte, musste das Verwaltungsverfahren beim TLfDI abgeschlossen werden. Nach § 38 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) kann der TLfDI nur Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Eine Videokamera wurde vorliegend nicht angebracht, sodass kein Datenschutzverstoß festgestellt werden konnte. Jedoch stellen nach Auffassung des TLfDI die angebrachten Hinweisschilder möglicherweise einen Eingriff in das allgemeine Persönlichkeitsrecht der Passanten oder der Wartenden an der Bushaltestelle dar. Die Betroffenen können sich nicht sicher sein, ob sich

in der Nähe eine Kamera befindet, welche Aufnahmen macht, selbst wenn diese nicht zu sehen ist. So wird auch in diesem Fall aufgrund des Hinweisschildes ein gewisser Überwachungsdruck auf die Passanten ausgeübt, was letztendlich zu einem Eingriff in deren allgemeines Persönlichkeitsrecht führen kann. Es können daher möglicherweise zivilrechtliche Ansprüche der Betroffenen gegen den Eigentümer des Grundstücks bestehen.

Die Ermächtigungsbefugnis des TLfDI, Anordnungen zur Beseitigung von festgestellten Mängeln und Verstößen bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel zu treffen, ergibt sich aus § 38 Abs. 5 Satz 1 BDSG. Sofern kein datenschutzrechtlicher Verstoß seitens des TLfDI festgestellt werden kann, bedeutet dies nicht, dass nicht auch daneben bestehende zivilrechtliche Abwehransprüche im Rahmen der Verletzung des allgemeinen Persönlichkeitsrechts vorliegen können.

6.47 Betreiber einer Videoüberwachung? – Ja Nein Vielleicht; Videogaga 21

Eine Thüringer Stadtverwaltung (SV) bat den Thüringer Landesbeauftragten für den Datenschutz die die Informationsfreiheit (TLfDI) um Unterstützung und Aufklärung zu einer an einem Gebäude angebrachten Videoüberwachung. Nach Mitteilung der SV waren zwei Kameras am Gebäude angebracht. Das Gebäude gehörte wohl einer Privatperson. Außerdem hatte ein Unternehmen Räumlichkeiten im Gebäude angemietet. Die SV belegte dies durch entsprechende Auszüge aus dem Grundbuchamt und durch Fotos.

Der TLfDI wandte sich daraufhin mit einem Auskunftsverlangen gemäß § 38 Bundesdatenschutzgesetz (BDSG) an den Eigentümer, aber auch an das Unternehmen, um in Erfahrung zu bringen, wer letztlich Betreiber – und somit Eigentümer – der Kameras – und damit verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG – sei.

Das Unternehmen erklärte dem TLfDI, dass es nicht mehr Mieter in diesem Gebäude und damit auch nicht verantwortlich für die Betreibung der Kameras sei. Des Weiteren teilten es mit, dass die Kameras bereits vor seinem Einzug in das Gebäude installiert gewesen waren.

Der Eigentümer des Gebäudes nahm ebenfalls Stellung zum Auskunftsverlangen. Er erklärte, dass er zwar Eigentümer des Gebäudes sei, allerdings nicht Betreiber der Videoüberwachung.

Für den TLfDI war die Rechtslage aufgrund der vorliegenden Fakten undurchsichtig und er recherchierte weiter. Es musste letztlich geklärt werden, ob das Unternehmen nun noch Mieter ist oder nicht und wer die Kameras angebracht hatte. Es stellte sich zwar heraus, dass es ein gerichtliches Verfahren zwischen Vermieter und Mieter gab, in dessen Rahmen auch über die Mietzinsen gestritten wurde. Leider konnte auch hieraus nicht abgeleitet werden, wer die Kameras tatsächlich betreibt. Allerdings wurde vom Vermieter eingeräumt, dass die Kameras bereits vor Übergabe an den Mieter installiert waren. Auch war der Mieter nicht mehr im Objekt und hatte auch keine Möglichkeit mehr, auf die Kameras einzuwirken. Zwar wurde er im Zivilprozess zur Mietzinszahlung verurteilt, jedoch handelte es sich nur um Versäumnisurteile. Solche Urteile kommen dann zustande, wenn eine Partei, hier der Mieter, nicht zum Termin erscheint. Da es sich beim Zivilprozess um einen Parteienprozess handelt, werden somit nur noch die Ausführungen der anderen Partei auf Schlüssigkeit geprüft und auf dieser Grundlage wird der Prozess entschieden. Mit anderen Worten: Aus einem Versäumnisurteil lassen sich auch keine tatsächlichen Umstände ableiten, sondern es handelt sich nur um überprüfte Aussagen einer Partei.

Da der Mieter somit nicht mehr als verantwortliche Stelle in Betracht kam und der Vermieter in einem anderen Bundesland wohnte, gab der TLfDI das Verfahren an die Kollegen des anderen Bundeslandes ab und informierte diese über den Sachstand. Kurz darauf informierten die Kollegen des anderen Bundeslandes darüber, dass die Sache im Sinne des Datenschutzes geklärt wurde, jedoch ohne näher auf weitere Einzelheiten einzugehen.

Gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz i. V. m. § 38 Abs. 6 BDSG ist der TLfDI als sachlich zuständige Behörde zur Kontrolle der Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz ermächtigt, § 38 Abs. 1 Satz 1 BDSG. Allerdings richtet sich die örtliche Zuständigkeit nach den Verwaltungsverfahrensgesetzen der Länder. Befindet sich die verantwortliche Stelle außerhalb von Thüringen, dann sind in der Regel die Kollegen des anderen Landes zuständig. Ausnahmen gibt es nur bei selbstständigen Niederlassungen von Unternehmen. Hier kann der TLfDI

tätig werden, selbst wenn das Unternehmen seinen Hauptsitz in einem anderen Bundesland hat.

6.48 Geschützte Fassaden

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass an der Dachrinne eines Gebäudes eine Kamera installiert sei, die auch die öffentlichen Gehwege und die Straße erfasse.

Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdeführerin gewandt und bat um die Beantwortung eines Fragenkataloges.

Diese äußerte hierauf, dass es sich bei der an ihrem Haus angebrachten Kamera lediglich um eine Attrappe handle. Da sie im Erdgeschoss sehr große Fenster habe und einige ihrer Nachbarn bereits Opfer von Vandalismus geworden seien, habe sie die Kameraattrappe zu ihrem eigenen Schutz angebracht. Sie hoffe, damit gewaltbereite Täter abschrecken zu können. Dafür sei es erforderlich, dass die Dummy-Kamera einer echten Kamera täuschend ähnlich sähe.

Leider hatte sich die Angelegenheit damit noch nicht, wie sie annehm, erledigt.

Der TLfDI geht im Falle der Videoüberwachung davon aus, dass die Vorschriften des BDSG sinngemäß auch auf Kameraattrappen anzuwenden sind, weil der durch diese ausgelöste Überwachungsdruck dem einer funktionsfähigen Kamera entspricht und somit ein ähnlicher Eingriff in das Persönlichkeitsrecht vorgenommen wird wie durch eine tatsächlich funktionierende Kamera.

In einem für den Datenschutz als Meilenstein geltendem Urteil hatte das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde als Grundrecht anerkannt. Anlass für diese Entscheidung war ein Volkszählungsgesetz, mit welchem Daten von allen Bürgern gesammelt werden sollten.

Kernaussage dieses Urteiles ist Nachfolgendes:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist,

ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ (BVerfG, Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 [Volkszählungsurteil]).

Diese dort aufgestellten Grundsätze gelten auch für das Installieren von Kameraattrappen, da hier der Eindruck einer echten Kamera erweckt werden soll, sodass der Betroffene nicht weiß, wer was wann und bei welcher Gelegenheit über ihn weiß.

So hat das Landgericht Darmstadt entschieden, dass das Aufstellen einer funktionsfähig aussehenden Videokamera-Attrappe mit der Ausrichtung des Objektivs auf den Hauseingangsbereich eines Mehrparteienhauses und die darin liegende konkludente Androhung einer dauernden Videoüberwachung rechtswidrig das allgemeine Persönlichkeitsrecht der Mieter (und ihrer jeweiligen Besucher) verletzt (LG Darmstadt, Urteil vom 17. März 1999 Az. 8 O 42/99).

Daher bat der TLfDI die Beschwerdegegnerin, ihm mitzuteilen, welche Bereiche die von ihr installierte Kameraattrappe zu erfassen scheint.

Sie erwiderte, die am Haus angebrachte Kameraattrappe sei so ausgerichtet, dass sie den Anschein erwecke, die Fenster im Erdgeschoss zu erfassen. Eine Überwachung im öffentlich zugänglichen Bereich, hier von Fenstern und Fassade, ist nur unter bestimmten Umständen rechtlich zulässig. Insofern ist auch bei der Verwendung von Attrappen zu prüfen, ob die datenschutzrechtlichen Vorgaben zur Beobachtung dieser Bereiche nach § 6b BDSG eingehalten wer-

den. Die Anwendung der vorgenannten Norm setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich, wie vorliegend, um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen.

Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zulässig, soweit es zur Wahrnehmung des Hausrechts für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll – wie hier – die Videoüberwachung dazu eingesetzt werden, vor Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.

In ihrem Schreiben hatte die Beschwerdegegnerin solche Vorkommnisse genannt. Ziel der von ihr durchgeführten vermeintlichen Videoüberwachung mittels der Kameraattrappe sei die Verhinderung von Beschädigungen durch die abschreckende Wirkung der Kameraattrappe. Dieses Ziel stellt ein berechtigtes Interesse dar, dessen Zweck konkret festgelegt wurde. Die vermeintliche Videoüberwachung der Fassade mittels der Attrappe ist auch als erforderlich anzusehen. Sie ist geeignet, die von ihr genannten Zwecke zu erreichen und es ist kein Mittel ersichtlich, welches bei gleicher Zumutbarkeit weniger stark in die Rechte Dritter eingreifen würde.

Bei der Wahrnehmung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG endet die Beobachtungsbefugnis des Hausrechtinhabers grundsätzlich an den Grundstücksgrenzen. Daneben lässt die Rechtsprechung (vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) im Einzelfall zu, dass der öffentliche Verkehrsraum in einer Breite von bis zu einem Meter mitaufgenommen wird.

Dies konnte die Beschwerdegegnerin – bildlich dokumentiert – dadurch gewährleisten, indem sie – nach dem Hinweis des TLfDI – die Kameraattrappe deutlich näher (ein Meter) auf ihre Fassade ausrichtete. Damit war das Verfahren für den TLfDI beendet.

Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist regelmäßig zulässig. Die Beobachtungsbefugnis des Hausrechtinhabers im Sinne des Datenschutzes endet dabei grundsätzlich an

den Grundstücksgrenzen. Daneben lässt die Rechtsprechung je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter aufgenommen wird. Voraussetzung hierfür ist jedoch, dass ausreichend Ausweichfläche verbleibt, um der Videoüberwachung ausweichen zu können. Diese Grundsätze sind auch auf Kameraattrappen anzuwenden, weil der durch diese Kameras ausgelöste Überwachungsdruck denen funktionsfähiger Kameras entspricht und somit ähnliche Eingriffe in das Persönlichkeitsrecht vorgenommen werden wie durch tatsächlich funktionierende Kameras.

6.49 Die überwachte Datsche

Der Pächter einer Parzelle in einer Gartenanlage in Thüringen suchte das Gespräch mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er habe ein Problem mit einem Nachbarn, der glaube, sein Grundstück werde vom Anfragenden überwacht.

Auf dem von ihm näher beschriebenen Grundstück betreibe er eine Videoüberwachungsanlage, bestehend aus vier Kameras. Die Kameras seien zum Teil auch auf benachbarte Grundstücke ausgerichtet. Zwischen seiner Parzelle und der streitbefangenen Nachbarparzelle befände sich eine etwa zweieinhalb Meter hohe und einen Meter breite Hecke. Dahinter wiederum befände sich ein blickdichter Zaun. Seine Videoüberwachungsanlage beträfe zwar auch Teile der Nachbargrundstücke, ihr tatsächlicher Sichtbereich beschränke sich – aufgrund technischer Vorkehrungen an den Kameras – ausschließlich aber auf sein Grundstück. Der Himmel über der Hecke zum streitgegenständlichen Nachbargrundstück sei ebenso ausgeschwärzt wie die teilweise seitlich auch noch mit erfassten Nachbarparzellen. Von diesen Grundstücken sei kameratechnisch nicht das Geringste zu erkennen.

Als Beweis dafür legte er Dokumente vor, die dies bestätigen.

Nach der dem TLfDI dargebotenen Sachlage war die Videoüberwachungsanlage datenschutzkonform und von seiner Seite nicht zu beanstanden.

Den nicht im Fokus stehenden Teil des Erfassungsbereiches einer Kamera unkenntlich zu machen, kann auf verschiedenen Wegen erreicht werden. Diese Bereiche können zum einen auf digitaler

Ebene geschwärzt oder unscharf gemacht werden (verpixeln). Zum anderen kann dieser Bereich der Linse mechanisch entsprechend bearbeitet werden.

6.50 Hausrecht – Video

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde darauf aufmerksam gemacht, dass an einem Fenster im ersten Obergeschoss eines Gebäudes eine Videokamera angebracht ist, welche vermutlich auf den öffentlichen Bereich des Gehweges gerichtet ist.

Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Beschwerdegewerter gewandt und bat um die Beantwortung eines Fragenkataloges.

In Beantwortung dieser Fragen erläuterte der Betreiber der Anlage, dass er mit der für jedermann sichtbaren, installierten Videokamera die Fassade, sein Schaufenster und den Ladeneingang überwache. Dies belegte auch ein im Anhang beigefügter Screenshot, aufgenommen von der Videokamera. Öffentlich zugängliche Bereiche wie die angrenzende Straße waren geschwärzt. Die Videokamera sei nicht schwenkbar und habe keine Zoomfunktion. Es erfolge eine digitale Aufzeichnung auf einem Server, die nach drei Tagen automatisch überschrieben werde. Eine Auswertung finde nur nach Vorkommnissen statt. Als Zweck für die Installation der Videokamera führte er die Beweissicherung bei Diebstählen und Sachbeschädigungen an seinem Gebäude auf. Er sei in der Vergangenheit bereits mehrfach Opfer von Vandalismus, konkret von Graffiti-Schmierereien, sowie von Einbruchversuchen gewesen. Ein entsprechendes Hinweisschild auf die Videoüberwachung sei angebracht, was der TLfDI auch den beigefügten Bildern im Anhang zu seinem Schreiben entnehmen konnte.

Nach Sichtung der beigefügten Fotos wurde der angrenzende Gehweg und damit öffentlich zugänglicher Raum im Sinne des § 6b BDSG von der Videoüberwachungsanlage miterfasst. Aus den übersandten Aufnahmen ergab sich, dass der Aufnahmebereich des angrenzenden Gehweges zur Hausfassade lediglich einen Meter betrug und weitere öffentlich zugängliche Bereiche (Straße) vom Betreiber unkenntlich gemacht worden sind. Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwa-

chung zur Wahrnehmung des Hausrechts zulässig. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann repressive oder präventive Zwecke verfolgen, indem Personen beispielsweise davon abgehalten werden sollen, Rechtsverstöße – z. B. Sachbeschädigungen durch Graffiti bzw. Beschädigungen an Gebäuden sowie Einbrüche innerhalb des vom Hausrecht umfassten Bereichs – zu begehen. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis an die Grenzen des Grundstücks und nach der Rechtsprechung einen Meter darüber hinaus. Im Einzelfall muss die Beobachtungsbefugnis jedoch in geringem Umfang über die Grundstücksgrenze hinausgehen dürfen und einen Toleranzbereich mitumfassen, wenn dies einer effektiven Überwachung zum Schutze des Eigentumes dient (Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 [Aktenzeichen 16 C 427/02]). In diesem Urteil, welches für die Rechtsprechung in diesem Bereich der Videoüberwachung richtungsweisend war und allgemeine Geltung erfahren hat, hatte das erkennende Gericht einen Toleranzbereich von einem Meter ab der Hauswand als vertretbar erachtet.

Im Ergebnis sah der TLfDI die im Fenster installierte Videokamera, ausgerichtet auf die Fassade und den Ladeneingang, im Sinne des § 6b Abs. 1 Nr. 2 zur Wahrnehmung des Hausrechts als datenschutzrechtlich zulässig an. Sie war erforderlich und es bestanden keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen.

Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Dabei wird von einer Lösungsfrist von 48 Stunden ausgegangen. In seiner Stellungnahme führte der Beschwerdegegner aus, dass die Daten erst nach drei Tagen automatisch überschrieben werden.

Nachdem er dem TLfDI mitgeteilt hatte, dass nunmehr eine Löschung binnen 48 Stunden erfolge, sah dieser das Verwaltungsverfahren als erledigt an.

Das Hausrecht umfasst die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Die Berufung auf das Hausrecht ist datenschutzkonform, wenn es für dessen Wahrung erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Spätestens an Grundstücksgrenzen jedoch endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel. Darüber hinaus wurde mit Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 (Aktenzeichen 16 C 427/02) entschieden, dass eine Videoüberwachungsanlage einen 1 Meter breiten Streifen entlang der Straßenseite sowie einen 1 Meter breiten Streifen links und rechts der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen dürfe.

6.51 Mein schöner Garten!

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Beschwerdegegner auf ihrem Hausgrundstück eine Videoüberwachungsanlage mit drei Kameras betreiben sollen. Alle drei Kameras seien so ausgerichtet, dass sie auch öffentlich zugängliche Bereiche überwachten.

In ihrer daraufhin vom TLfDI erbetenen Stellungnahme haben die Beschwerdegegner eingeräumt, eine solche Anlage auf ihrem Grundstück installiert zu haben. Sie sei aber ausschließlich auf ihr Grundstück gerichtet, sodass kein öffentlich zugänglicher Bereich, sondern nur ihr Garten von der Anlage betroffen sei. Sie hätten die Anlage angebracht, nachdem es mehrfach zu Verletzungen ihrer Persönlichkeits- und Eigentumsrechte gekommen sei. Nach den Einlassungen der Beschwerdegegner handelt es sich bei den Kameras um solche, die zwar geeignet seien, Bilder zu erzeugen und zu speichern, aber aufgrund fehlender Hard- und Software dazu (noch) nicht fähig seien. Bisher seien die Kameras lediglich Attrappen. Die Beschwerdegegner planten in der Folge jedoch, die Anlage „in Funktion“ zu setzen. Vor der „Scharfschaltung“ der Anlage beabsichtigten die Beschwerdegegner, den TLfDI in die Beratung hinsichtlich der Positionierung der einzelnen Kameras miteinzubeziehen. Das angekündigte Miteinbeziehen war bis zum Erstellen dieses Berichtes noch

nicht erfolgt. Aufgrund des Zeitablaufes wird der TLfDI bei den Beschwerdegegnern abklären, wann die „echte“ Inbetriebnahme der Anlage nunmehr geplant ist.

Unabhängig vom Vorstehenden sollte auch bei Verwendung von Attrappen bedacht werden, dass diese ebenfalls in das Persönlichkeitsrecht Dritter eingreifen.

Insoweit wird der TLfDI die oben angeführte Nachfrage nach dem Zeitpunkt der Inbetriebnahme der Anlage mit dem Begehrt um Über-sendung von Lichtbildern der Kameras sowie der jeweiligen Erfas-sungsbereiche verbinden und seine Prüfung sodann fortsetzen.

In allen Bereichen, in denen sich der Einsatz „echter“ Kameras ver-bietet, sollte auch der Einsatz von Kameraattrappen kritisch besehen werden, da in diesen Fällen eine Verletzung des Persönlichkeits-rechts Dritter ebenso vorliegen kann.

6.52 Video bleibt datenschutzrechtlich schwierig!

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und be-schwerte sich über eine Videoüberwachungsanlage seines Nachbarn. Die Kameras seien wohl so ausgerichtet, dass das Grundstück des Beschwerdeführers und öffentlicher Bereich miterfasst würde.

Der TLfDI wandte sich daraufhin mit einem Auskunftersuchen nach § 38 Bundesdatenschutzgesetz (BDSG) an den Nachbarn (im Fol-genden „Betreiber“ genannt). Diesem wurde mitgeteilt, dass durch eine Videoüberwachungsanlage personenbezogene Daten erhoben und – im Falle einer gleichzeitigen Speicherung der Aufnahmen – auch verarbeitet werden. Dies sei aber nur dann zulässig, wenn dies durch das BDSG oder eine andere Rechtsvorschrift erlaubt wäre. Eine Möglichkeit zur Zulässigkeit dieser Videoüberwachung wäre die Einwilligung des Betroffenen nach § 4 Absatz 1 BDSG. Bei einer Videoüberwachung ist eine Einwilligung allerdings nur schwer ein-zuhalten, da nicht absehbar ist, welche Personen zu welchem Zeit-punkt in den Erfassungsbereich der Videoüberwachung gelangen könnten. Bei der Überwachung des eigenen Grund und Bodens ist die Zulässigkeit einer Videoüberwachung unter bestimmten Voraus-setzungen zulässig. Dies ist der Fall, wenn die Erhebung, Verarbeit-ung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG und keine Per-

sonen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Außerdem hat der Betreiber darauf zu achten, dass sich der Erfassungsbereich der Videoüberwachung ausschließlich auf sein eigenes Grundstück richtet.

Der Betreiber bestätigte die Videoüberwachungsanlage und erklärte, dass dies nur zur Abschreckung von Einbrechern diene. Er möchte sich und sein Grundstück schützen. Der Betreiber kooperierte von Anfang an mit dem TLfDI und übersandte detailliertes Bildmaterial von den angebrachten Kameras.

Anhand der übersandten Unterlagen und des Bildmaterials wurde seitens des TLfDI festgestellt, dass eine der Kameras in einer Höhe angebracht ist, in welcher das Filmen des Nachbargrundstücks möglich war. Der Betreiber wurde daraufhin gebeten, diese Kamera so zu versetzen und dies durch Bilder nachzuweisen, dass eine mögliche Aufnahme des Nachbargrundstücks ausgeschlossen werden kann. Der Betreiber kam dieser Aufforderung auch prompt nach. Somit blieb für den TLfDI noch einzig die Prüfung der Kamera am Hauseingangsbereich. Hierzu wurde dem Betreiber mitgeteilt, dass diese Kamera nur dann zulässig ist, sofern ausgeschlossen wird, dass andere Personen erfasst werden. Denn mithilfe der Videoüberwachungsanlage im Hauseingangsbereich wäre es möglich, andere Personen, wie zum Beispiel den Postboten, zu filmen. Zwar ist der Hauseingangsbereich als öffentlich zugänglicher Raum zu betrachten, allerdings würden die schutzwürdigen Interessen der Betroffenen gemäß § 6b BDSG gegen das ausgeübte Hausrecht grundsätzlich nicht überwiegen, sofern auf die Videoüberwachungsanlage hinreichend hingewiesen wird. Durch die Bildnachweise wurde seitens des TLfDI festgestellt, dass sich der Briefkasten und auch die Klingel am Eingangstor befinden. Somit gelangt kein Postbote zwangsläufig in den Erfassungsbereich der Videoüberwachungsanlage. Ebenso hatte der Betreiber ein entsprechendes Hinweisschild angebracht.

Somit waren die Kameras und deren Ausrichtungen mit dem Datenschutz vereinbar.

Der Betreiber bedankte sich für die Hinweise.

Eine Videoüberwachung des eigenen und allein genutzten Grundstückes ist grundsätzlich zulässig. Jedoch nur dann, wenn gemäß § 1 Absatz 2 Nummer 3 BDSG die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätig-

keiten erfolgt und keine Personen, die nicht in einem persönlichen oder familiären Verhältnis zum Betreiber stehen, von der Videokamera erfasst werden können. Zwar wäre es möglich den Postboten oder Besucher zu filmen, das Hausrecht überwiegt allerdings nach § 6b BDSG an der Stelle.

6.53 Alle Wege führen zum Kindergarten: Videogaga 22

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfahren, dass auf dem Grundstück der Beschwerdegegner zwei Kameras mit Blickrichtung auf einen Weg bzw. die Straße angebracht worden seien. Der Weg werde als Zugang für den Gemeindekindergarten genutzt. Er sei zwar im Eigentum der Beschwerdegegner, es bestehe aber ein Wegerecht für den dahinterliegenden Kindergarten.

Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdegegner gewandt und um die Beantwortung eines standardisierten Fragenkataloges gebeten.

Auf die Anfrage bestätigten die Beschwerdegegner die Installation der Kameras. Der Gemeinde diene der streitgegenständliche Weg als Zuwegung zu ihrem Kindergarten. In den letzten Jahren sei es mehrfach dazu gekommen, dass Eltern unberechtigtweise mit ihren Fahrzeugen die Einfahrt der Beschwerdeführer genutzt hätten, um zum Kindergarten zu fahren oder ihre Fahrzeuge in der Einfahrt abzustellen. Zudem gäbe es auf dem Grundstück des Kindergartens keine ausreichende Umzäunung, sodass viele Bewohner den Weg wochentags und auch am Wochenende benutzten, um auf den Spielplatz zu gehen. Der Gemeinde sei diese Problematik schon länger bekannt. Der eigentliche Grund zum Betreiben einer Videoüberwachungsanlage sei jedoch der Schutz des Eigentums gegen Vandalismus, Einbruch und Diebstahl.

Die Videoüberwachungsanlage sei noch nicht in Betrieb, solle künftig aber den angesprochenen Bereich überwachen. Die Beschwerdegegner möchten als Eigentümer ihr Eigentum schützen, keinesfalls hätten sie jedoch ein Interesse, Unbeteiligte zu überwachen. Zur Dokumentation der Vorfälle möchten sie eine Festplatte installieren. In seiner Erwiderng bekräftigte der TLfDI, dass es grundsätzlich einer Rechtsvorschrift bedarf, die eine solche Videoüberwachung

erlaubt, es sei denn, es handele sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen.

Eine ausschließlich private oder familiäre Tätigkeit war vorliegend nicht gegeben. Das von den Kameras der Beschwerdeführer erfasste Spektrum umfasst auch öffentliche Bereiche, weswegen das BDSG vorliegend einschlägig und der TLfDI für den oben genannten Sachverhalt damit zuständig ist. Die Richtlinie zum Schutz personenbezogener Daten ist auf die Videoaufzeichnung mit einer Überwachungskamera anwendbar, die von einer Person an ihrem Einfamilienhaus angebracht wurde und auf den öffentlichen Straßenraum gerichtet ist (vgl. EUGH, Urteil C-212/13 vom 11. Dezember 2013). Das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts bemisst sich nach § 6b Abs. 1 Nr. 2 BDSG. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis an die Grenzen des Grundstücks bzw. einen Meter jenseits der Grundstücksgrenzen, wenn dies zur Wahrnehmung des Hausrechtes erforderlich ist und keine schutzwürdigen Interessen Dritter überwiegen.

Weder Kamera 1 noch Kamera 2 beobachteten damals nur das im Eigentum der Beschwerdegegner stehende Grundstück, sondern auch den mit einer Nutzungsvereinbarung belasteten Weg zum Kindergarten außerhalb ihres Grundstücks bzw. die öffentliche Straße (mehr als einen Meter). Das Eigentum am Grundstück begründet jedoch kein Recht an einer Videoüberwachung anderer berechtigter Grundstücksnutzer im Hinblick auf die Ausübung ihres Wegerechts.

Nach den Ausführungen der Beschwerdegegner kam es ihnen beim Aufstellen der Kameras entscheidend auch darauf an, den Weg zum Kindergarten mitzuerfassen, sodass ein Verstellen des Betrachtungswinkels oder Schwärzen des Aufnahmebereiches keine Alternativen darstellten.

Das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts begründet daher vorliegend nicht dessen Zulässigkeit.

Nach § 6b Abs. 1 Nr. 3 BDSG ist das Beobachten öffentlich zugänglicher Räume mit einer Videoüberwachung nur zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung, wie vorliegend, dazu eingesetzt werden, vor Einbruch und Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.

Die Gefährdungslage muss substantiiert dargelegt werden. Diesem Erfordernis haben die Beschwerdegegner nicht Rechnung getragen. Im Ergebnis musste der TLfDI feststellen, dass die von den Beschwerdegegnern betriebenen Kameras unzulässig sind.

Die Beschwerdegegner haben die Ausführungen des TLfDI nachvollziehen können und haben datenschutzrechtlich zulässige Zustände geschaffen.

Nach § 6b Abs. 1 Nr. 3 BDSG ist das Beobachten öffentlich zugänglicher Räume mit einer Videoüberwachung zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbruch, Diebstahl und Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit.

6.54 Bewachter Parkplatz

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis erlangt, dass ein Anwohner an der

Fassade seines Wohnhauses eine Kamera angebracht hat, die auch den öffentlich zugänglichen Bereich überwache.

Daraufhin hat der TLfDI dem Antragsgegner einen Fragebogen zugesandt, in dem dieser dem TLfDI unter anderem erklären sollte, ob er auf seinem Grundstück eine Kamera installiert habe.

Der Beschwerdegegner teilte dem TLfDI mit, dass er in der Tat eine Kameraattrappe auf seinem Grundstück angebracht habe. Diese Kamera sei aber ausschließlich auf sein Grundstück gerichtet. Die Attrappe sei von ihm angebracht worden, um seine – vor der Toreinfahrt und noch auf seinem Grundstück – geparkten Autos vor Vandalismus zu schützen. Es sei schon mehrfach zu Übergriffen auf diese gekommen und er wisse, wer dafür verantwortlich gewesen sei. Leider hätte er dies nicht beweisen können. Seit der Installation der Kamera habe es keine weiteren Vorfälle dieser Art gegeben.

Aus den dem Schreiben beigelegten Unterlagen, dem Lageplan und den Fotos zur Örtlichkeit und der Kameraattrappe selbst wurde für den TLfDI ersichtlich, dass der Beschwerdegegner – entgegen den Ausführungen des Beschwerdeführers – tatsächlich nur das eigene Grundstück überwachte.

Nach § 6b Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) ist das Beobachten öffentlich zugänglicher Räume mittels Videoüberwachung zur Wahrnehmung des Hausrechts zulässig. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann repressive oder präventive Zwecke verfolgen, indem Personen beispielsweise davon abgehalten werden sollen, Rechtsverstöße – z. B., wie vorliegend, Sachbeschädigungen an den Fahrzeugen des Beschwerdegegners innerhalb des vom Hausrecht umfassten Bereichs – zu begehen. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis zur Grundstücksgrenze bzw. in Ausnahmefällen einen Meter darüber hinaus (Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 – Aktenzeichen 16 C 427/02).

Da die Überwachung lediglich das Grundstück des Beschwerdegegners erfasste und keine Anhaltspunkte ersichtlich waren, dass

schutzwürdige Interessen anderer überwiegen, sah der TLfDI den Vorgang als erledigt an.

Das Videoüberwachen öffentlich zugänglicher Räume kann nach § 6b Abs. 1 Nr. 1 BDSG zulässig sein. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen. Diese Beobachtungsbefugnis reicht jedoch lediglich bis zur Grundstücksgrenze bzw. in Ausnahmefällen einen Meter darüber hinaus.

6.55 Planung einer Videoüberwachung – der TLfDI hilft auch hier

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wegen der Anbringung von Kameraattrappen an einem Gebäude, welches aufgrund der Lage an einem Weltkulturerbe touristisch hochfrequentiert war, angefragt. Das Haus wurde vom Eigentümer gerade frisch saniert. Es kam kurz nach der Sanierung zu Graffiti-schmierereien an dem Gebäude. Diese konnten zwar wieder entfernt werden, jedoch befürchtete der Eigentümer eine Verwahrlosung der Umgebung um das Gebäude, da in dem Treppenaufgang neben dem Haus Schäden durch das Urinieren von Personen entstanden waren. Der TLfDI machte sich im Rahmen eines Vor-Ort-Termins ein Bild von der Umgebung, um eine entsprechende Beratung durchzuführen. Es sollten insgesamt drei Kameraattrappen an der Hausfassade angebracht werden, um eine abschreckende Wirkung hinsichtlich der eingetretenen Beschädigungen zu erzielen.

Dabei sollten zum einen eine Kameraattrappe an der Rückseite des Gebäudes und zwei an der Hauswand zum Treppenaufgang installiert werden. Dieser Treppenaufgang befand sich zwischen den Gebäuden und war lediglich einen Meter breit.

Nach Auffassung des TLfDI stellen auch Attrappen einen Eingriff in das vom Bundesverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung dar. Daher sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) einzuhalten.

Ferner wurde der Eigentümer des Gebäudes darauf hingewiesen, dass auch bei Kameraattrappen, welche, wie in diesem Fall, öffentlich zugängliche Räume erfassen, ein Hinweisschild auf die Videoüberwachung anzubringen ist. Entsprechend § 6b Abs. 2 BDSG ist dieses Hinweisschild in Augenhöhe anzubringen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die verantwortliche Stelle, welche die Videokameras angebracht hat, erkennbar sein. Daher ist sie grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen. Der Eigentümer des Hauses wurde durch den TLfDI umfassend zu allen Voraussetzungen für eine Installation von Kameras beraten. Bei einem Vor-Ort-Termin mit dem Eigentümer wurden nochmals die möglichen Kamerastandorte in Augenschein genommen und ihre möglichen Erfassungsbereiche sowie die mögliche Beeinträchtigung der Passanten abgeklärt. Der Eigentümer hat sich am Ende aber doch nicht für die Installation von Kameras an dem Gebäude entschieden.

Nach Auffassung des TLfDI stellt auch eine Kameraattrappe einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Diese können nicht wissen, ob die Kamera tatsächlich Aufnahmen macht oder ob es sich lediglich um ein Kameragehäuse handelt. Daher löst auch eine solche Kameraattrappe einen Überwachungsdruck bei den Betroffenen aus.

6.56 Nette Familie

Die Beschwerdeführer wandten sich gegen eine von einem männlichen Familienmitglied installierte Kamera, mittels derer er das von ihnen gemeinsam genutzte und bewohnte Grundstück beobachtete. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat den Betreiber der Anlage u. a. um Auskünfte, welche Bereiche zu welchen Zwecken und seit wann videoüberwacht, auf welche Art und Weise die erhobenen Daten gespeichert und wie lange die Überwachungsdaten aufbewahrt werden.

Daraufhin teilte der Beschwerdegegner mit, dass es sich bei dieser Kamera um eine Attrappe handele, die weder aufzeichnen noch spei-

chern könne. Aufgestellt sei diese nur zur Abschreckung wegen einiger Diebstähle auf seinem Grundstück.

Nach der Auffassung des TLfDI ist der von einer Attrappe ausgelöste Überwachungsdruck dem einer funktionsfähigen Kamera ähnlich, weil damit auch ein Eingriff in die Persönlichkeitsrechte der Betroffenen vorgenommen wird.

Datenschutzrechtlich war die Kamera durch den TLfDI allerdings nicht zu beurteilen. Da der scheinbare Aufnahmebereich der hier streitgegenständlichen Kameraattrappe ausschließlich auf das im Eigentum des Beschwerdegegners befindliche Grundstück gerichtet war und die Aufnahmen ausschließlich zu privaten oder familiären Zwecken diene, war das BDSG nicht anwendbar, § 1 Abs. 2 Nr. 3 BDSG.

Damit musste der TLfDI die Angelegenheit als erledigt ansehen.

Handelt es sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG. Danach findet das Gesetz keine Anwendung auf die Verarbeitung personenbezogener Daten, die eine natürliche Person zur ausschließlich persönlichen Verwendung vornimmt. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher oftmals nicht nach dem BDSG zu beurteilen.

6.57 Kamerainstallation oder nicht, das ist hier die Frage

Im Berichtszeitraum hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis davon erlangt, dass ein Bürger auf einem in der Anzeige näher benannten Grundstück auch öffentliche Flächen mit seinen Videokameras überwache.

Im Zuge der Ermittlungen übersandte der TLfDI dem Beschwerdegegner als verantwortlicher Stelle einen Fragebogen zur Beantwortung der genaueren Angaben über die (vermeintliche) Videoüberwachung des Beschwerdegegners verlangte.

In seiner Rückantwort wies der Beschwerdegegner die Behauptung, auf seinem Grundstück eine Videoüberwachung durchzuführen, zurück. Auf diesem Grundstück seien weder Kameras noch Kameraattrappen installiert.

Bei der Wahrnehmung seiner aufsichtsbehördlichen Tätigkeit ist der TLfDI mitunter darauf angewiesen, fremde Hilfe in Anspruch zu

nehmen. § 5 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) regelt die Voraussetzungen und Grenzen der Amtshilfe auf Behördenebene. Die dort an die Amtshilfe gestellten Voraussetzungen waren vorliegend gegeben.

Gemäß § 38 Thüringer Datenschutzgesetz haben öffentliche Stellen die Pflicht, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Deshalb wandte sich der TLfDI nochmals an das Ordnungsamt, das ihn seinerzeit auf die Existenz der Kameras hingewiesen hatte, und bat es, die gerügten Kameras zu fotografieren und ihm die entsprechenden Bilder zu übersenden.

Zum Zeitpunkt der Erstellung dieses Berichts war die erbetene Fotodokumentation von den strittigen Kameras noch nicht zur Akte gelangt.

Das weitere Vorgehen des TLfDI hängt von dem Befund ab, der sich aus den noch zu überreichenden Aufnahmen ergibt.

Eine Behörde – vorliegend der TLfDI – kann um Amtshilfe insbesondere dann ersuchen, wenn sie aus rechtlichen Gründen die Amtshandlung nicht selbst vornehmen kann, aus tatsächlichen Gründen, wenn die zur Vornahme der Amtshandlung erforderlichen Dienstkräfte oder Einrichtungen fehlen, sie die Amtshandlung nicht selbst vornehmen kann, sie zur Durchführung ihrer Aufgaben auf die Kenntnisse von Tatsachen angewiesen ist, die ihr unbekannt sind und die sie selbst nicht ermitteln kann, sie zur Durchführung ihrer Aufgaben Urkunden oder sonstige Beweismittel benötigt, die sich im Besitz der ersuchten Behörde befinden, sie die Amtshandlung nur mit wesentlich größerem Aufwand vornehmen könnte als die ersuchte Behörde.

Weiterhin ist gemäß dem Thüringer Datenschutzgesetz die Unterstützung durch die öffentlichen Stellen verpflichtend.

6.58 Ich glaub, ich steh im Wald

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da er beabsichtige, eine Wildkamera zum Filmen und Fotografieren von Tieren auf dem eigenen Grundstück zu installieren. Abhängig davon, an welcher Stelle er die Kamera anbringe, sei es möglich, dass auch eine Teilfläche des Nachbargrundstücks miterfasst werde. Außerdem

fragte er sich, ob der Sachverhalt anders zu beurteilen sei, wenn er sicherstelle, dass ausschließlich das eigene Grundstück betroffen ist. Er sei sich über die geltende Rechtslage unsicher.

Der TLfDI ist auch für die Einhaltung der datenschutzrechtlichen Gesichtspunkte bei der Videoüberwachung zuständig, weswegen er sich der Fragen annahm.

Bei einer Videoüberwachung handelt es sich immer um einen Umgang mit personenbezogenen Daten. Diese ist nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt, anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Das Erheben, Verarbeiten oder Nutzen der mit einer Wildkamera erstellten Aufnahmen stellen automatisierte Verarbeitungen dar, sofern hiervon personenbezogene Daten betroffen sind.

Die Zulässigkeit des Einsatzes von Wildkameras durch nicht-öffentliche Stellen, worunter Privatpersonen (z. B. Jäger) fallen, beurteilt sich grundsätzlich nach § 6b BDSG, wenn öffentlich zugänglicher Raum erfasst wird.

Der vorgeschilderte Sachverhalt ist den Fällen ähnlich, in denen Wildkameras im „klassischen“ Wald aufgestellt werden, mit dem Unterschied, dass hier der Fokus auf der Beobachtung des eigenen Grundstückes liegt.

Bei der Beurteilung der Zulässigkeit von Videokameras, die auf Grundstücken angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Es bedarf einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn es handelt sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG (Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13). Entscheidend ist hierbei, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Der Anwendungsbereich der vorgenannten Entscheidung ist eng auszulegen. Daher kann eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet, nicht als eine „ausschließlich persönliche oder familiäre Tätigkeit“ angesehen werden.

Die Überwachung des allein genutzten Grundstücks jedoch ist regelmäßig zulässig. Die sich daraus ergebende Beobachtungsbefugnis endet allerdings an der Grundstücksgrenze.

In der ersten Fallgestaltung, in der der Fragensteller nicht ausschließen konnte, dass neben seinem Grundstück auch das Nachbargrundstück von der Beobachtung betroffen werde, kommt eine ausschließlich private oder familiäre Tätigkeit nach der vorgenannten Rechtsprechung nicht in Betracht.

Nach § 6b Abs. 1 BDSG kann eine Videoüberwachung zulässig sein, soweit sie der Wahrnehmung des Hausrechts oder der Wahrnehmung berechtigter Interessen dient.

Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts unter Berücksichtigung der Erforderlichkeit und der Interessenabwägung zulässig, sofern sie nur an die Grenzen des Grundstücks bzw. je nach Einzelfall maximal einen Meter darüber hinaus erfolgt. Diese Grenze ist bei der ersten Fallgestaltung überschritten.

Die vom Anfragenden betriebene Videoüberwachung ist daher im Falle der Mitüberwachung des Nachbargrundstücks von § 6b Abs. 1 Nr. 2 BDSG nicht gedeckt.

Deshalb kommt in diesem Falle eine Zulässigkeit nach § 6b Abs. 1 Nr. 3 BDSG in Betracht. Danach ist eine Videoüberwachung öffentlich zugänglicher Räume zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Daneben muss die Videoüberwachung auch erforderlich sein, um diesen Zweck zu erreichen. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann. Deswegen muss man sich mit zumutbaren Alternativen auseinandersetzen, die in das informationelle Selbstbestimmungsrecht des Einzelnen weniger eingreifen. Eine reine Aufzeichnung ist für präventive Zwecke nicht geeignet, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Live-Monitoring gegeben, da der Betreiber dort unmittelbar eingreifen kann.

Soweit eine Erforderlichkeit für die Videoüberwachung zur Wahrung eines berechtigten Interesses vorliegt, darf sie nur in Betrieb

genommen werden, wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Betreibers und den von der Überwachung Betroffenen vorzunehmen. Die permanente Überwachung stellt einen gravierenden Eingriff dar und führt häufig dazu, dass deutliche Anhaltspunkte dafür vorliegen, dass schutzwürdige Interessen der betroffenen Personen gegenüber den berechtigten Interessen des Betreibers überwiegen.

Sowohl die erste als auch die zweite Sachverhaltsschilderung sind zu wenig konkret, um eine abschließende Beurteilung zu ermöglichen. Um belastbare Aussagen über die Zulässigkeit der Kameras treffen zu können, wären weitere Angaben notwendig gewesen, die aufgrund der Abstraktheit der Anfrage nicht vorgelegen haben.

Sofern sich die Videoüberwachung ausschließlich auf das eigene Grundstück bezieht und nur Bereiche erfasst, die nicht zum Betreten durch Dritte vorgesehen sind, ist eine Videoüberwachung aus datenschutzrechtlicher Sicht regelmäßig zulässig, da dort das BDSG überhaupt keine Anwendung findet.

6.59 Problemzonen im Autohaus – Fortsetzung

Bereits im 1. Tätigkeitsbericht im nicht-öffentlichen Bereich wurde unter Punkt 3.17 ausführlich über eine datenschutzrechtliche Kontrolle eines Autohauses berichtet; ein Ergebnis dazu gab es leider in dem Berichtszeitraum 2012/2013 nicht.

Zum Hintergrund: Gegenstand einer datenschutzrechtlichen Kontrolle des TLfDI war ein Autohaus. Im Nachgang der Kontrolle gab es einige Punkte, die datenschutzrechtlich bewertet werden mussten. Unter anderem betrieb das Autohaus umfangreich eine Videoüberwachungsanlage im öffentlich zugänglichen Außenbereich des Autohauses. Da nach § 4 Abs. 1 BDSG das Erheben, Nutzen und Verarbeiten von personenbezogenen Daten nur zulässig ist, wenn es hierzu einen Norm gibt, die dies anordnet oder erlaubt oder der Betroffene eingewilligt hat, waren die Voraussetzungen des § 6b BDSG zu prüfen, der abschließend die Überwachung von öffentlich zugänglichen Räumen regelt. Nur wenn eine Videoüberwachung diesen Anforderungen entspricht, ist sie aus datenschutzrechtlicher Sicht zulässig.

Das Autohaus betrieb die Videoüberwachungsanlage, da es in der Vergangenheit bereits zu mehreren Diebstählen, Einbrüchen und Sachbeschädigungen gekommen war. Die Vorkommnisse wurden auch bei der Polizei gemeldet und konnten als Nachweis für ein berechtigtes Interesse der Videoüberwachung nach § 6b Abs. 1 Nr. 3 BDSG gewertet werden. Der TLfDI sah allerdings die Videoüberwachung nicht als erforderliches Mittel zur Vermeidung der Delikte an und verlangte vom Autohaus, dass ein milderer Mittel eingesetzt wird, mit dem die genannten Vorkommnisse (Diebstahl, Einbrüche, Sachbeschädigungen) vermieden werden können. Hierzu wäre der Einsatz von Monitoring möglich gewesen. Ein zuständiger Mitarbeiter könnte – bei einer oben dargestellten Situation – somit dann gleich eingreifen. Das Autohaus argumentierte, dass es nicht in der Lage sei, sein Personal mit der zusätzlichen Aufgabe des Monitorings zu beschäftigen. Zu umfangreich seien die Bereiche, die auf dem Gelände des Autohauses videoüberwacht werden. Hinzu komme der Kostenfaktor für die Variante. Außerdem sei es auch ein berechtigtes Interesse, Schadensersatzforderungen im Nachhinein durchsetzen zu können.

Im Ergebnis sah der TLfDI deswegen die Videoüberwachungsanlage unter den dargestellten Gründen als zulässig an, legte dem Autohaus allerdings nahe, über den Einsatz von Monitoring nachzudenken und Sicherheitspersonal für die Überwachung des Monitoring zu beauftragen. Das Sicherheitspersonal könnte sofort eingreifen, wenn etwas passiert. So würden Beschädigungen verhindert.

Jede datenschutzrechtliche Würdigung ist eine Einzelfallentscheidung. In diesem Fall ist man nach zwei Tätigkeitsberichtszeiträumen zu einem Ergebnis gekommen. Im Fokus der datenschutzrechtlichen Prüfung war der § 6b BDSG, von dem eine Voraussetzung nach § 6b Abs. 1 Nr. 1 bis 3 BDSG hätte erfüllt sein müssen, damit die Videoüberwachung im öffentlich zugänglichen Bereich zulässig ist. Sollte von Unternehmen Videoüberwachungsanlagen installiert werden, ist dringend erforderlich, dass die gesetzlichen Grenzen der Zulässigkeit solcher Maßnahmen geprüft und nicht überschritten werden. Bei allgemeinen Anfragen verweist der TLfDI immer auf die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises, in der die Grundsätze zulässiger Videoüberwachung aufgeführt sind. Diese Orientierungshilfe stellt der TLfDI auf seiner Website

(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_nicht-ffentliche-stellen.pdf) zur Verfügung.



6.60 Ob der Lkw richtig steht, sieht man, wenn die Kamera angeht – Videogaga 23

Bei einer datenschutzrechtlichen Kontrolle wurde eine durch eine Firma betriebene Videoüberwachung seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) überprüft. Auf dem Firmengelände konnten zwei Videokameras festgestellt werden. Beide Kameras waren auf die Lkw-Waage gerichtet und dienten der Kontrolle, ob der Lkw richtig auf der Waage platziert war. Der Monitor war im Waagenraum angebracht. Die Kameras zeichneten nicht auf und waren nur zu den Geschäftszeiten eingeschaltet. Sie waren nicht schwenk- und zoomfähig. Es gab jedoch kein Hinweisschild, welches auf die Videoüberwachung in diesem Bereich hingewiesen hat.

Die Zulässigkeit der betreffenden Videoüberwachung richtete sich in diesem Fall nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Danach ist das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Der von der verantwortlichen Stelle vorgetragene Zweck, zu kontrollieren, ob der Lkw richtig auf der Waage platziert wurde, war als konkret festgelegter Zweck im Rahmen des berechtigten Interesses zu berücksichtigen. Hinsichtlich der Erforderlichkeit der Videoüberwachung ergaben sich ebenfalls keine Bedenken. Darüber hinaus gab es keine Anhaltspunkte, dass schutzwürdige Interessen Betroffener, in diesem Fall die be-

berechtigten Interessen der Firma, überwiegen. Zu bemängeln war jedoch, dass nicht auf die Videoüberwachung im Bereich der Lkw-Waage hingewiesen wurde. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grds. mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen. Der Mangel wurde seitens der verantwortlichen Stelle umgehend behoben und ein den Vorgaben des § 6b Abs. 2 BDSG entsprechendes Hinweisschild im Bereich der Videoüberwachung wurde angebracht. Die Videoüberwachung wird nach Einschreiten des TLfDI nunmehr datenschutzkonform betrieben.

Die gebotene Hinweispflicht gem. § 6b Abs. 2 BDSG im Rahmen der Videoüberwachung in öffentlich zugänglichen Bereichen dient insbesondere dazu, den Betroffenen die Möglichkeit zu geben, dass diese selbst entscheiden können, der Überwachung auszuweichen oder ihr Verhalten entsprechend anpassen zu können. Deswegen ist es wichtig, dass die verantwortlichen Stellen diese Hinweispflicht ernst nehmen und auch erfüllen. Der Hinweis kann mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist etwa in Augenhöhe anzubringen. Die für die Datenverarbeitung verantwortliche Stelle muss erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grds. mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

Achtung: Bisher führte ein fehlender Hinweis weder zu einem Bußgeld, noch zu einer Rechtswidrigkeit der Videoüberwachung selbst. Dies wird sich mit Geltung der Datenschutz-Grundverordnung (DS-GVO) ab Ende Mai 2018 ändern. Verstöße gegen die dort genannten Informationspflichten können zu empfindlichen Geldbußen (bis zu 20 Mio. Euro) führen. Im Rahmen der Bestimmung der Höhe dieser Geldbußen sind jedoch z. B. Art, Schwere und Dauer des Verstoßes sowie weitere in Art. 83 Abs. 1 DS-GVO aufgeführte Vorgaben zu berücksichtigen. Darüber hinaus führt ein Mangel bei diesen Informationspflichten zur Rechtswidrigkeit der Videoüberwachung.

6.61 Streetview outsourced – davon wird's nicht besser; Videogaga 24

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und wollte wissen, ob er „Probleme“ bekommen würde, wenn er Fotos vom öffentlichen Straßenverkehr ins Internet hochladen würde. Die Kamera würde in sehr kurzen Zeitintervallen auslösen. Er gibt an, dass die von ihm bevorzugte Seite zwar Personen und Autokennzeichen verpixeln würde, es aber wohl bei Automatismen dieser Art üblich sei, dass dies nur selten zu 100 Prozent passiert. Dies würde bedeuten, dass ein Gesicht oder Autokennzeichen eventuell sichtbar bzw. leserlich sein könnte. Weiterhin erklärte er, dass die Fotos zum Zwecke der geografischen sowie straßenverkehrstechnischen Datenermittlung genutzt werden würden, um eben das Programm als freie und offene Geodatenbank verbessern zu können.

Der TLfDI teilte dem Bürger daraufhin mit, dass er tatsächlich „Probleme“ bekommen könnte, wenn er solche Fotos hochladen würde, nämlich dann, wenn er dabei erwischt wird und der TLfDI davon Kenntnis bekäme. Eine bezweckte Dauerbeobachtung öffentlich zugänglicher Räume ist mit dem Bundesdatenschutzgesetz (BDSG) nicht vereinbar. Die Beobachtung, worunter auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt, von öffentlich zugänglichen Räumen fällt, wozu der öffentliche Straßenverkehr gehört, hat der Gesetzgeber in § 6b BDSG abschließend geregelt. Danach ist eine Beobachtung von öffentlich zugänglichen Räumen nur dann zulässig, wenn dies zur Aufgabenerfüllung durch öffentliche Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwe-

cke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse. Nur unter diesen genannten Voraussetzungen sind solche Videoüberwachungen zulässig. Diese waren in dem vorgenannten Fall nicht gegeben. Wird eine solche Datenerhebung durchgeführt, ohne dass die Voraussetzungen von § 6b BDSG vorliegen, erfüllt dies den Ordnungswidrigkeitentatbestand des § 43 Abs. 2 Nr. 1 BDSG. Dieser kann mit einem Bußgeld geahndet werden.

Eine bezweckte Dauerbeobachtung öffentlich zugänglicher Räume ist mit dem Bundesdatenschutzgesetz (BDSG) nicht vereinbar. Eine Beobachtung durch Dritte von öffentlich zugänglichen Räumen, wozu auch der Straßenverkehr gehört, hat der Gesetzgeber in § 6b BDSG abschließend geregelt.

6.62 Die (Un)zulässigkeit von Dashcams oder Die Leiden des (jungen) Hobbyfilmers

Die Zulässigkeit von sogenannten Dashboardcams bzw. Dashcams, dies sind in Fahrzeugen installierte Kameras, mit denen das Verkehrsgeschehen aufgenommen wird und die so gewonnenen Bilder gespeichert werden können, ist umstritten. Bei den auch als „Armaturenbrett-Kameras“ bezeichneten Aufnahmegeräten steht ein Aufklärungsinteresse, zumeist von Unfallbeteiligten, dem Persönlichkeitsrecht der anderen Verkehrsteilnehmer gegenüber. Während in verschiedenen Ländern deren Einsatz rechtlich zulässig oder verboten ist, ist in Deutschland die Rechtslage noch unklar. Während die Datenschützer deren Einsatz mehrheitlich als datenschutzwidrig ansehen, gibt es in Deutschland zu deren Zulässigkeit bzw. Unzulässigkeit noch keine gefestigte Rechtsprechung. Da sich der Einsatz solcher Kameras stetig größerer Beliebtheit erfreut, ist auch der Kreis der Urteile, die sich mit der Rechtmäßigkeit dieser Kameras befassen, deutlich gestiegen.

Die nach hiesiger Meinung bekanntesten Urteile, die sich mit diesem Thema beschäftigen sind:

- Amtsgericht München, Urteil vom 9. August 2017 Az. 1112 OWi Js 121012/17
- Amtsgericht München, Urteil vom 6. Juni 2013 Az. 343 C 4445/13
- Amtsgericht Nienburg, Urteil vom 20. Januar 2015, Az. 4 Ds 520 Js 39473/14
- Landgericht Landshut, Hinweisbeschluss vom 1. Dezember 2015, Az.12 S 2603/15
- Oberlandesgericht Stuttgart, Beschluss vom 4. Mai 2016, Az. 4 SS 543/15
- LG München I, Beschluss vom 14. Oktober 2016, Az.: 17 S 6473/16
- Verwaltungsgericht Ansbach, Urteil vom 12. August 014, Az. AN 4 K 13.01634
- Amtsgericht München, Hinweisbeschluss vom 13. August 2014, Az. 345 C 5551/14
- Landgericht Heilbronn Urteil vom 17. Februar 2015 Az. I 3 S 19/14
- Landgericht Memmingen Urteil vom 14. Januar 2016 Az. 22 O 1983/13.
- Verwaltungsgericht Göttingen Urteil vom 31. Mai 2017 Az.1 A 170/16

Während sich die ersten fünf Entscheidungen für die (partielle) Zulässigkeit von Dashcams im Sinne einer gerichtlichen Verwertbarkeit aussprechen, negieren die übrigen Entscheidungen deren grundsätzliche Zulässigkeit. Mit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, in dem Datenschutz, dem sog. Recht auf informationelle Selbstbestimmung, Verfassungsrang zuerkannt wurde, hat sich das bis dahin geltende Datenschutzrecht grundlegend geändert. Als Bundesgesetz ist das Bundesdatenschutzgesetz allseits, d. h. auch im Zivilrecht, im Strafrecht und im Ordnungswidrigkeitsrecht, zu beachten.

Die zitierten Entscheidungen, die den Einsatz partiell als legitim ansehen, begründen dies teilweise auch damit, dass der Gesetzgeber lediglich die fest installierten Kameras in den Geltungsbereich von § 6b Bundesdatenschutzgesetz (BDSG) einbezogen habe.

Diese Entscheidungen, die die Rechtmäßigkeit der Videoüberwachung mittels Dashcams befürworten, sehen dies unter dem Blickwinkel der Beweisverwertung gegebenenfalls auch rechtswidrig erlangter Beweise im Zivil-/Strafprozess bzw. Ordnungswidrigkeitsverfahren.

Besonders das Urteil des Amtsgerichtes München, Urteil vom 6. Juni 2013 (Az. 343 C 4445/13) wurde als Anerkennung für den Einsatz von Dashcams gewertet, weil dort erstmals ein deutsches Zivilgericht die Frage der Verwertung der mithilfe einer Dashcam gefertigten Aufnahmen positiv entschieden hat. Die Frage der Zulässigkeit bei der Verwertung derartiger Aufnahmen bestimme sich nach Interessen beider Parteien, die gegeneinander abzuwägen wären. Im dort entschiedenen Fall war ein Autofahrer in einen Verkehrsunfall verwickelt. Zum Zeitpunkt der Aufnahme sei noch keine Zweckbestimmung erfolgt. Die Personen, die auf Video aufgenommen worden waren, seien rein zufällig ins Bild geraten. Eine Beeinträchtigung von Grundrechten läge nur dann vor, wenn eine derartige, zufällig gewonnene Aufnahme im Nachgang gegen den Willen der abgebildeten Person veröffentlicht werde. Wegen der (nachträglichen) Beweiserheblichkeit könnten solche Aufnahmen im anschließenden Prozess durchaus Verwendung finden.

Nach dem Urteil des Amtsgerichtes Nienburg sei die Vorschrift § 6b BDSG nicht anwendbar, da diese Norm nur für den ortsfesten Betrieb einer Kamera gelte. Dieser Schluss ergebe sich bereits aus der Hinweispflicht nach § 6b Abs. 2 dieser Vorschrift. Beim Betrieb einer beweglichen Kamera sei es schlicht unmöglich, die betroffenen Personen auf bevorstehende Aufzeichnungen hinzuweisen. Dies wiederum sei Voraussetzung für die Anwendung dieser Vorschrift. Im konkreten Falle sei die hier erfüllte spezialgesetzliche Ermächtigung, die dem Zeugen das Videoaufzeichnen ermögliche, die entsprechende Anwendung des § 28 Abs. 1 Nummer 1 BDSG. Bei der Kommentierung dieses Urteils wird oftmals übersehen, dass das erkennende Gericht die Verwertbarkeit als Beweis im Strafverfahren nur in sehr engen Grenzen gebilligt hat. Der Zeuge, der das Unfallgeschehen dort aufgenommen hat, hatte die Kamera nicht dauernd im Einsatz sondern nur als Beweismittel in der konkreten strafrechtlich relevanten Situation. In dieser kurzen, anlassbezogenen Aufnahme waren zudem auch keine Personen, sondern nur das Auto des Täters zu sehen.

Nach Ansicht des Landgerichts Landshut seien Videoaufnahmen mit Dashcams grundsätzlich verwertbar. Das Anfertigen der Aufnahmen sei nicht verboten, weswegen auch kein Beweisverwertungsverbot bestehe. Das Kunsturhebergesetz (KUG), welches unter anderem das Recht am eigenen Bild schütze, sei nach Auffassung des Landgerichtes nicht einschlägig. Abgesehen davon, dass die von der Aufnahme Betroffene selbst nicht videografiert worden sei, verbiete § 22 KUG nur das Verbreiten und Präsentieren von Aufnahmen, nicht aber das Aufnehmen selbst. Auch das Bundesdatenschutzgesetz hielt das erkennende Gericht für unanwendbar. Diese Norm gelte lediglich für fest installierte Kameras. Zwar habe das Verwaltungsgericht Ansbach das anders gesehen, aber der Fall dort habe anders gelegen. In diesem oben angeführten Urteil des Verwaltungsgerichtes Ansbach habe der Kläger systematisch den Verkehrsraum überwacht, um dann Anzeigen wegen Ordnungswidrigkeiten zu erstatten.

Selbst ein Verstoß gegen das Bundesdatenschutzgesetz hätte aus Sicht des Gerichtes nicht zu einem Beweisverwertungsverbot geführt. Das laufende Filmen des Verkehrsgeschehens durch eine On-board-Kamera stelle keinen gravierenden Grundrechtseingriff dar. Eventuell abgebildete Personen blieben anonym. Ohnehin müsse jeder Autofahrer zwingend damit rechnen, dass seine Fahrweise von anderen beobachtet werde. Zwar komme den Filmaufnahmen nach einem Unfall eine größere Bedeutsamkeit zu. Aber nach einem Unfall würden ständig die Fahrzeuge, die Unfallspuren und auch umstehende Beteiligte zwecks Beweissicherung fotografiert werden.

Die oben angeführte Entscheidung des Oberlandesgerichtes Stuttgart hat es, zumindest für den Bereich der Verfolgung schwerwiegender Ordnungswidrigkeitenverfahren, für zulässig erachtet, mit einer Dashcam aufzunehmen. Bei dieser Entscheidung hat das Gericht offen gelassen, ob bzw. unter welchen Voraussetzungen der Einsatz einer Dashcam durch einen anderen Verkehrsteilnehmer gegen § 6b BDSG verstoße. Jedenfalls enthalte § 6b Abs. 3 Satz 2 dieser Norm kein Beweisverwertungsverbot für das Straf- und Bußgeldverfahren. Ein für das Gericht möglicher Verstoß gegen das Datenschutzgesetz sei nicht zwingend ein Grund, die Aufnahmen nicht zu verwerten. Über deren Verwertbarkeit sei vielmehr im Einzelfall unter Abwägung der widerstreitenden Interessen zu entscheiden.

Auch das Landgericht München I sah in der oben aufgeführten Entscheidung eine Verwertung der Aufnahmen im Zivilprozess – unter umfassender Abwägung der Interessen des Abgebildeten an einer

selbstbestimmten Verwendung personenbezogener Datensätze einerseits und dem Beweissicherungsinteresse des Beweisführers andererseits – als möglich an, wenn diese Aufnahmen nur anlassbezogen erstellt würden und sichergestellt sei, dass diese Aufnahmen nach einer bestimmten Zeit gelöscht oder überschrieben würden.

Zu einem anderen Ergebnis kommt das Landgericht Heilbronn in seinem oben angesprochen Urteil. Aufzeichnungen einer in einem Pkw installierten Dashcam könnten im Zivilprozess wegen eines Beweismittelverbotes nicht als Beweismittel zum Hergang eines Unfalls verwertet werden. Eine solche großflächige Beobachtung von öffentlichen Straßen stelle schon deshalb einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen dar, weil durch die hier vorgenommene, permanente Aufzeichnung mit der Videokamera eine Vielzahl von Personen in kurzer Zeit in ihrem allgemeinen Persönlichkeitsrecht betroffen wird.

Das Landgericht Memmingen hat in seinem Urteil das Anfertigen von Videoaufnahmen von Personen im öffentlichen Straßenraum als rechtswidrig angesehen, wenn dies durch eine an der Windschutzscheibe eines Pkw installierte betriebsbereite Dashcam geschähe. Dies gelte auch dann, wenn diese über einen Bewegungsmelder verfüge, soweit die Aufzeichnungen nicht ausnahmsweise erforderlich wären und das schutzwürdige Interesse des Verwenders der Kamera überwöge. Soweit die Befürworter der Zulässigkeit von Dashcams im Straßenverkehr ins Feld führten, die Vorschrift des § 6b BDSG sei nur auf stationäre Kameras anzuwenden, sei dem nicht zu folgen. Diese Auslegung sei dem Gesetzeswortlaut nicht zu entnehmen. Zudem werde die Beobachtung entgegen § 6b Abs. 2 BDSG auch nicht in geeigneter Weise deutlich gemacht. Ein kleines Warnschild im Pkw genüge insoweit nicht, da es nicht ins Auge steche und erst aus großer Nähe sichtbar sei.

Einen ganz besonderen Fall hatte das Verwaltungsgericht Göttingen zu entscheiden. Dort hatte ein Rentner seine Dashcam dazu benutzt, seine privaten „Ordnungsfantasien“ auszuleben. Der als „Knöllchen-Horst“ in die Geschichte eingegangene Ordnungshüter hatte mehr als 15.000 Verkehrsverstöße dokumentiert und bei den Verfolgungsbehörden angezeigt. Das Gericht kam zu dem Schluss, dass der Einsatz von Dashcams im öffentlichen Verkehrsraum sowohl die Persönlichkeitsrechte der Verkehrsteilnehmer wie auch den Datenschutz verletze. § 6b BGSg verbiete es, ohne dort genannte Gründe personenbezogene Aufnahmen zu fertigen. Ein Verstoß gegen diese Norm

läge schon deshalb vor, weil der Anzeigenerstatter den Umstand der Beobachtung nicht erkennbar gemacht habe. Die permanente Überwachung des Verkehrs sei darüber hinaus auch nicht gerechtfertigt gewesen, da er mit seinem Verhalten keine schützenswerten Eigeninteressen verfolgt habe, sondern Sachwalter öffentlicher Interessen sei.

In Polizeikreisen wird die Zulässigkeit von Dashcams durchaus befürwortet. Sie könnten zum Nachweis von Verkehrsstraftaten dienen, bei denen bisher als Beweismittel allenfalls Aussagen und Erinnerungen vorlägen. Die Gewerkschaft der Polizei plädiert deswegen für eine verbindliche Einführung eines sogenannten Unfalldatenspeichers.

Im Sinne der Rechtsklarheit ist es zwingend geboten, eine verbindliche Regelung zu schaffen, die die widerstreitenden Interessen der Beteiligten berücksichtigt. Es ist nicht von der Hand zu weisen, dass das Beweisinteresse der die Kameras nutzenden Verkehrsteilnehmer einerseits und ein Interesse der übrigen Verkehrsteilnehmer zur Wahrung der Persönlichkeitsrechte andererseits im Widerstreit stehen. Dieser Widerstreit muss schnellstens aus Gründen der Rechtssicherheit aller Beteiligten gelöst werden.

In Deutschland fehlt es bisher an einer verbindlichen Regelung dazu, ob und bejahendenfalls in welchem Maße Dashcams für den Straßenverkehr genutzt werden können.

6.63 Nicht alle Wege führen zum Friedhof

Ein Beschwerdeführer wandte sich wegen einer am Waldesrand installierten Kamera an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Der Besitzer eines Waldstückes und der umliegenden Grundstücke verweigere anderen mittels dieser Kamera faktisch die Nutzung des sich auf diesem Areal befindlichen Weges zum Friedhof, weil diese sich – zutreffend – beobachtet fühlten. Dieser streitgegenständliche Weg sei in der Katasterkarte eingetragen und erfreue sich großer Beliebtheit. Wahrscheinlich, um seinen Wunsch nach dessen Nichtgebrauch zu überwachen und zu sehen, wer diesen Weg gleichwohl nutze, habe er eine Beobachtungskamera an einem dort befindlichen Baum in ca. 3,50 Meter Höhe installiert.

Der TLfDI hat daraufhin dem Besitzer des streitbefangenen Grundstückes ein Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) zugesandt und um die Beantwortung eines Fragenkataloges gebeten.

Darauf erwiderte der Beschwerdegegner, dass er auf dem vom TLfDI genannten Grundstück keine funktionstüchtige Videoüberwachungsanlage betreibe. Auch werde von ihm nicht der Eindruck erweckt, dort eine Videoüberwachungsanlage zu betreiben.

Das zuständige Landratsamt hat den TLfDI inzwischen darüber informiert, dass die streitbefangene Kamera zwischenzeitlich deinstalliert wurde.

Damit hat sich die Angelegenheit für den TLfDI erledigt.

Der Betreiber einer Videoüberwachungsanlage ist nach § 38 Abs. 3 BDSG verpflichtet, unverzüglich, vollständig und wahrheitsgemäß seiner Auskunftspflicht nachzukommen. Wenn der Auskunftspflichtige dieser Verpflichtung vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, handelt er nach § 43 Abs. 1 Nummer 10 BDSG ordnungswidrig. Die Ordnungswidrigkeit kann nach § 43 Abs. 3 Satz 1 BDSG mit einer Geldbuße bis zu 50.000 € geahndet werden.

6.64 Rundumüberwachung durch den Nachbarbetrieb?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über drei installierte Videokameras an einem Privat- und Firmengelände. Eine der Kameras erfasste wohl ausschließlich das Privatgrundstück. Die beiden anderen waren auf den öffentlichen Verkehrsraum ausgerichtet, womit auch teilweise das Haus der Beschwerdeführerin mit Zufahrtsweg sowie das Grundstück eines weiteren Nachbarn erfasst waren. Der TLfDI wandte sich mit einem Auskunftersuchen an den Betreiber der Kameras. Dieser teilte mit, dass keine Aufzeichnung über die Videokamera erfolgte, sondern nur eine Beobachtung mittels Bildübertragung auf einen Monitor stattfand. Die Kameras dienten der Kontrolle der Zufahrt zum Grundstück (Wohnbereich und Betrieb) als auch der Überwachung des Betriebsgeländes, da dort Gefahrgut gelagert war.

Durch die „reine“ Beobachtung mit optisch-elektronischen Einrichtungen werden ebenfalls personenbezogene Daten erhoben. Nach § 4

Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Vorliegend kamen hier entweder § 6b BDSG oder § 28 Abs. 1 Nr. 2 BDSG in Betracht, um die Zulässigkeit der Videoüberwachung zu beurteilen, abhängig davon, welche Bereiche erfasst wurden.

§ 28 Abs. 1 Nr. 2 BDSG gilt für nicht-öffentlich zugängliche Bereiche. Nicht-öffentlich zugänglich sind Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Entscheidend ist hierbei, dass die Nicht-Öffentlichkeit durch Verbotsschilder oder den Kontext der Umgebung erkennbar ist. Danach ist das Erheben von personenbezogenen Daten als Mittel zur Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Anhand der im Auskunftsverfahren erteilten Informationen und Bilder und der Aufnahmewinkel der Kameras war erkennbar, dass das gesamte Grundstück eingezäunt und ohne Einverständnis des Besitzers nicht betreten werden konnte. Kamera 1 war nur auf das eigene Grundstück ausgerichtet und diente der Wahrnehmung des Hausrechts des Betreibers mittels Kontrolle unbefugten Betretens des Grundstücks. Ein berechtigtes Interesse zum Betreiben der Kameras lag daher vor. Auch konnten die Erforderlichkeit bejaht und das Überwiegen schutzwürdiger Interessen ausgeschlossen werden. Somit wurde diese Kamera vom TLfDI als zulässig betrachtet.

Allerdings erfassten die beiden anderen Kameras auch weite Bereiche des öffentlichen Verkehrsraums sowie Grundstücksbereiche der umliegenden Nachbarn.

§ 6b BDSG regelt die Videoüberwachung von öffentlich zugänglichen Räumen. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Ebenso handelt es sich um eine Überwachung von öffentlich zugänglichen Räumen, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden.

Gem. § 6b Abs. 1 Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Vi-

deoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Kameras dienten wie bei Kamera 1 der Kontrolle des Zutritts zum Grundstück, also zur Wahrnehmung des eigenen Hausrechts. Allerdings muss die Videobeobachtung auch für den festgelegten Zweck geeignet und erforderlich sein. Bewertet wird hier auch, wie die Videotechnik eingesetzt wird (insbesondere der räumliche Umfang). Beide Kameras beobachteten einen umfangreichen Bereich außerhalb des Grundstückes. Das ist für den festgelegten Zweck, Wahrnehmung des Hausrechts, nicht erforderlich. Darüber hinaus bestanden Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen. Durch die eingestellten Kamerawinkel werden unter Umständen eine Vielzahl von Fußgängern und auch Nachbarn beobachtet. Dies bedeutet einen erheblichen Eingriff in deren informationelles Selbstbestimmungsrecht. Bei einer Abwägung der Interessen des Überwachenden und der Beobachteten musste der Zweck der Wahrnehmung des Hausrechts insoweit zurückstehen.

Die Kameras müssen im Rahmen der Erforderlichkeit so positioniert sein, dass lediglich ein Bereich bis einen Meter hinter der Grundstücksgrenze aufgenommen wird. Selbst dies ist nur dann zulässig, wenn ausreichender Platz zum Ausweichen verbleibt. Zur Wahrnehmung des Hausrechts darf der öffentliche Verkehrsraum grundsätzlich nicht mit Videokameras überwacht werden.

Der Betreiber der Kameras folgte den Anweisungen des TLfDI. Er beschränkte den Aufnahmebereich einer Kamera mit einem Sichtschutz, sodass der öffentliche Verkehrsraum und das Nachbarhaus nicht mehr erfasst wurden. Die andere Kamera deinstallierte der Betreiber, da er eine Beobachtung dieses Bereichs auch durch ein Fenster vornehmen konnte. Die verbleibenden Kameras werden durch Einschreiten des TLfDI datenschutzkonform betrieben.

Auch mit einer reinen Videobeobachtung, also keiner Speicherung der Daten, werden personenbezogene Daten erhoben. Demnach benötigt eine solche Anlage gem. § 4 BDSG eine Berechtigung zum Betreiben dieser Kameras. Die Zulässigkeitsprüfung wird dann anhand von § 28 BDSG für nicht-öffentliche Bereiche oder § 6b BDSG für öffentlich zugängliche Bereiche vorgenommen.

6.65 Wertvoller Schrott im Fokus – Fortsetzung

Bereits im 1. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich wurde über eine Kontrolle eines Recycling-Unternehmens in Thüringen berichtet (Beitrag 3.12 im 1. Tätigkeitsbericht nicht-öffentlicher Bereich). Schwerpunkt der Kontrolle war, dass dieses Unternehmen eine Videoüberwachungsanlage an jeweils vier Standorten im Unternehmen betreibt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat bereits ausführlich die gesetzliche datenschutzrechtliche Sicht dargelegt, insbesondere, dass die Einhaltung des § 6b Bundesdatenschutzgesetz (BDSG) beim Einsatz von Videoüberwachungsanlagen in öffentlich zugänglichen Bereichen maßgeblich ist. Ein endgültiges Ergebnis konnte im genannten Berichtszeitraum nicht mitgeteilt werden, da das Verwaltungsverfahren beim TLfDI noch nicht abgeschlossen war.

Für Unternehmen, die Videoüberwachungsanlagen betreiben wollen, sind die Voraussetzungen nach § 6b Abs. 1 Nr. 2 bis 3 BDSG maßgebend. Nach § 6b Abs. 1 Nr. 2 BDSG ist eine Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gleiches gilt für § 6b Abs. 1 Nr. 3 BDSG. Hiernach ist eine Videoüberwachung nur zulässig, wenn sie zur Wahrung eines berechtigten Interesses für einen konkreten Zweck erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der TLfDI hielt drei der vier Kameras für datenschutzrechtlich zulässig. Die vierte Kamera war allerdings so ausgerichtet, dass im Kassenbereich nicht nur personengezogene Daten von Kunden erhoben wurden, sondern auch die sich an der Kamera aufhaltenden Mitarbeiter (u. a. der Kassierer) sowie zwei Arbeitsplätze gesehen werden konnten. Wie bereits im zweiten Absatz erwähnt, ist eine Videoüberwachung nach § 6b BDSG nur zulässig, wenn das berechtigte Interesse für konkret festgelegte Zwecke erforderlich ist und das schutzwürdige Interesse des Betroffenen nicht überwiegt. Die Videoüberwachung wurde vom Betroffenen als verantwortliche Stelle zu Sicherheitszwecken und zur Abschreckung eingesetzt. Dies kann grundsätzlich ein berechtigtes Interesse für einen konkret festgelegten Zweck darstellen. Zulässig wäre die Videoüberwachung aber nur

dann, wenn sie dafür auch erforderlich wäre und keine Anhaltspunkte dafür bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Zunächst entfaltet eine reine Videoüberwachung mittels aufzeichnender Kamera keine präventive Wirkung. Zwar können möglicherweise Vorkommnisse aufgeklärt werden, jedoch handelt es sich dabei um eine repressive Wirkung. Die wirksame Verhinderung z. B. von Diebstählen kann damit nicht bewerkstelligt werden. Die Art der Videoüberwachung ist daher nicht erforderlich. Demgegenüber steht das schutzwürdige Interesse der Kunden und der Mitarbeiter. Der Kunde hält sich im Kassenbereich auf, um seine Rechnung zu bezahlen. Er ist zudem gezwungen, diesen Bereich auch zu betreten. Auch der Kassierer läuft aus dienstlichen Gründen an der Kamera vorbei. Die Videoüberwachung im Kassenbereich stellt einen erheblichen Eingriff in die Privatsphäre des Kunden und der Mitarbeiter dar. Daraufhin forderte der TLfDI den Betreiber auf, dass die Videoüberwachungsanlage im Kassenbereich nur während der Schließzeiten aufzeichnet und dass während der Geschäftszeiten nur Live-Monitoring mit Verpixelung der Arbeitsplätze erfolgt. Das Unternehmen ist den Forderungen des TLfDI nachgekommen, indem es die Kamera im Kassenbereich außer Betrieb genommen hat.

Sollten von Unternehmen Videoüberwachungsanlagen installiert werden, ist dringend erforderlich, dass die gesetzlichen Grenzen der Zulässigkeit solcher Maßnahmen geprüft und nicht überschritten werden. Gern steht der TLfDI in solchen Fragen beratend zur Seite. Zur Rechtsgrundlage des § 6b BDSG gibt es auch eine „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Internetseite des TLfDI zur Verfügung steht: (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v_-durch-nicht-ffentliche-stellen.pdf).



6.66 Videoüberwachung als Auszugsgrund?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist durch die Beschwerdeführerin darauf aufmerksam gemacht worden, dass der Beschwerdegegner in einem Bürofenster eines Grundstückes eine Kamera installiert habe. Diese Kamera beobachte sowohl den Eingangsbereich des dort vom Beschwerdegegner unterhaltenen Büros wie auch die im selben Objekt befindliche Wohnung der Beschwerdeführerin.

Auf Nachfrage des TLfDI äußerte der Beschwerdegegner, im streitbefangenen Objekt tatsächlich eine Kamera positioniert zu haben. Er habe sie installiert, weil in der Gegend vermehrt eingebrochen worden sei. Die Kamera sei lediglich auf sein Grundstück, den Büroeingang, Teile des Innenhofes und die Garagenzufahrt gerichtet. Die Kamera sei nicht funktionstüchtig, da eine Speicherkarte derzeit noch nicht eingesetzt sei. Zukünftig aber sei eine Inbetriebnahme der Anlage angestrebt.

Nach weiterem Schriftverkehr stellte sich heraus, dass die streitgegenständliche Kamera lediglich auf sein – komplett von einer Mauer umgebenes – Grundstück ausgerichtet war. Dieses konnte zudem nach seinen Angaben nur nach manueller Betätigung des Eingangsportes betreten werden. Eine gewerbliche Nutzung des Objektes sei zwischenzeitlich aufgegeben worden.

Die Videoüberwachung in solchen Bereichen ist nur im Rahmen einer Erforderlichkeit des abschließenden Zweckkatalogs des § 6b Abs. 1 Nr. 1 bis 3 Bundesdatenschutzgesetz (BDSG) zulässig. Danach ist die Videoüberwachung nur statthaft, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Im vorliegenden Fall war – zumindest bei Einreichen der Beschwerde – die Beobachtungsbefugnis zur Wahrnehmung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG einschlägig.

Als berechtigtes Interesse hatte der Beschwerdegegner vorgetragen, die Überwachung seines Grundstückes sei notwendig, da es in der Umgebung zu Einbrüchen gekommen sei. Hierin ist die Wahrnehmung des eigenen Hausrechts zu sehen, welches die Befugnis beinhaltet, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des

Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen. Eine Beobachtung zur Wahrnehmung des Hausrechts dient sowohl einem präventiven als auch einem repressiven Zweck, indem zum einen Straftaten durch Abschreckung verhindert und zum anderen die Strafverfolgung durch die Beweissicherung ermöglicht werden soll. Auf den vom Beschwerdegegner übersandten Fotos ist zu erkennen, dass lediglich sein eigener Grundstücksbereich überwacht wird, sodass der räumliche Umfang der Überwachung für den Zweck der Wahrnehmung des Hausrechts nicht zu beanstanden ist.

Wenn bei der Videoüberwachung Anhaltspunkte bestehen, dass schutzwürdige Interessen von betroffenen Personen überwiegen, ist sie als unzulässig einzustufen. Dies könnte vorliegend der Fall sein, wenn – nicht mit dem Betreiber der Anlage in persönlicher oder familiärer Tätigkeit verbundene Dritte – das Grundstück nutzen, da deren schutzwürdige Interessen das berechtigte Interesse an der Wahrnehmung des Hausrechts häufig verdrängen.

Da die Beschwerdeführerin zum Zeitpunkt ihrer Beschwerde ebenfalls in dem Streitobjekt gewohnt hatte, sah sie sich in ihrem Persönlichkeitsrecht verletzt. Ob im vorliegenden Fall das Hausrecht zur Statthaftigkeit der Anlage geführt hätte, war nicht mehr zu entscheiden, nachdem die Beschwerdeführerin ihrerseits ausgezogen war. Daher bestanden keine Anhaltspunkte mehr dafür, dass schutzwürdige Interessen anderer von der Kamera verletzt würden.

Wenn bei der Videoüberwachung Anhaltspunkte bestehen, dass die schutzwürdigen Interessen von betroffenen Personen überwiegen, ist sie als unzulässig einzustufen. Dies ist beispielsweise der Fall, wenn auch nicht mit dem Betreiber der Anlage in persönlicher oder familiärer Tätigkeit verbundene Dritte ein Grundstück nutzen, da deren schutzwürdigen Interessen die berechtigten Interessen des Hausrechtsinhabers an der Wahrnehmung dieses Hausrechtes häufig verdrängen.

6.67 Videoüberwachungskamera auf der anderen Straßenseite

Das Ordnungsamt einer Stadtverwaltung meldete dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Videoüberwachungsanlage an einem gemischt genutzt-

ten Gebäude. Eine Videokamera war im 2. Stock des Hauses angebracht, sodass nicht ausgeschlossen werden konnte, dass die öffentliche Straße und Gehwege sowie die gegenüberliegenden Grundstücke vom Kamerabereich miterfasst wurden.

Der Hausbesitzer und gleichzeitige Geschäftsführer der dort ansässigen Firma wurde vom TLfDI angeschrieben und um Auskunft gebeten. Er teilte mit, dass es sich bei den drei angebrachten Kameras um Kameragehäuse (sog. Attrappen) handelte. Auf die „vermeintliche“ Kameraüberwachung wurde mit einem Schild hingewiesen. Weiter führte er aus, dass die Attrappen zur Verhinderung von weiteren Diebstählen, Einbrüchen und Vandalismus dienen würden. Zusätzlich hatte er ebenfalls eine akustische Alarmanlage installiert. Auf der gegenüberliegenden Straßenseite befand sich das Lager der Firma. Die Kameraattrappe im 2. Stock sollte dazu dienen, dieses Grundstück zu erfassen, da eine Attrappe an der Lagerhalle in den Augen des Betreibers nicht zielführend gewesen wäre und potenziell Straftäter diese entfernt oder zugeklebt hätten.

Nach Auffassung des TLfDI stellen auch Attrappen einen Eingriff in das vom Bundesverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung dar. Daher sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) einzuhalten.

Bezüglich einer der Kameraattrappen, die auf den Vorgartenbereich gerichtet war, äußerte der TLfDI keine Bedenken. Der Kamerawinkel war so ausgerichtet, dass lediglich das eigene Grundstück erfasst wurde und sie konnte daher auch bei einer nicht mehr konkret vorliegenden Gefahrensituation, im Rahmen der Wahrnehmung des eigenen Hausrechts, weiterhin genutzt werden.

Die anderen Kameraattrappen waren so ausgerichtet, dass sie letztendlich öffentlich zugängliche Bereiche miterfassten. Bei der im Erdgeschoss befindlichen Kameraattrappe bestanden Anhaltspunkte, dass die schutzwürdigen Interessen von Betroffenen überwiegen, da diese auf den Eingangsbereich der Büroräume gerichtet war. Kunden, Brief- und Paketzusteller mussten sich somit zwangsweise in den beobachteten Bereich begeben und hatten keine Ausweichmöglichkeiten hinsichtlich des Erfassungsbereichs der Kameraattrappe. Die andere Attrappe im 2. Stock des Gebäudes war für den von dem Betreiber genannten Zweck, mögliche Einbrecher abzuschrecken, nicht geeignet. Aufgrund der Position ist diese für potenzielle Täter nicht erkennbar, da diese meist nur die nähere Umgebung absuchen. Außerdem wurde an dem Gebäude eine akustische Alarmanlage

angebracht. Die Ausführungen des Hausbesitzers belegen, dass die vorgefallenen versuchten Einbrüche durch die Alarmanlage verhindert wurden und nicht durch die angebrachte Kameraattrappe auf der anderen Straßenseite.

Daraufhin entfernte der Hausbesitzer alle drei Kameraattrappen.

Auch eine Videoattrappe stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, da diese nicht wissen, ob die Kamera tatsächlich Aufnahmen macht oder es sich lediglich um ein Kameragehäuse handelt. Daher löst auch eine Kameraattrappe einen Überwachungsdruck bei den Betroffenen aus.

6.68 Apotheken-Video – Videogaga 25

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde bezüglich einer Videoüberwachung in den Verkaufsräumen einer Apotheke.

Der TLfDI ist nach § 42 Abs. 1 Thüringer Datenschutzgesetz i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) die nach § 38 Abs. 1 BDSG zuständige Aufsichtsbehörde für die Kontrolle der Einhaltung des BDSG sowie sonstiger datenschutzrechtlicher Vorschriften bei nicht-öffentlichen Stellen.

Im Rahmen dieser Zuständigkeit wandte sich der TLfDI mit einem Auskunftersuchen nach § 38 Abs. 3 BDSG, das einen Fragenkatalog zu der Videoüberwachungsanlage enthielt, an den Apotheker. Zudem sollten der Beantwortung auch Nachweise beigefügt werden, wie zum Beispiel ein Lageplan des Ladens mit den eingezeichneten Standorten der Kameras und Screenshots, aus denen sich der Aufnahmebereich der Kameras erkennen lässt.

Daraufhin teilte der Apothekenbesitzer dem TLfDI mit, dass es sich bei den zwei Kameras nur um Attrappen handele, die zur Abschreckung von potenziellen Ladendieben dienten. Diese seien auf beiden Seiten der Verkaufstheke befestigt, mit Ausrichtung zu den Kassensplätzen.

Da auch Attrappen einen Eingriff in das Persönlichkeitsrecht seiner Kunden begründen können, wies der TLfDI den Apotheker auf diese Rechtslage hin.

Der Apotheker entfernte daraufhin die Attrappen in seiner Apotheke.

Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz (§ 42 Abs. 1 S. 1 ThürDSG i. V. m. § 38 Abs. 6 BDSG). Um seiner Kontrollaufgabe nachgehen zu können, wurden dem TLfDI Kompetenzen verliehen. Hierzu gehört unter anderem, dass gem. § 38 Abs. 3 BDSG die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen haben. Wenn mit Vorsatz oder aus Fahrlässigkeit eine Auskunft unvollständig oder nicht rechtzeitig erteilt wird, kann dies mit einer Geldbuße geahndet werden.

6.69 Wenn der Thermenbesuch beobachtet wird – Videogaga 26

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr durch einen Hinweis von Kameraaufnahmen in einer Therme. Im Umkleidebereich der Sauna würden die Besucher gefilmt.

Der TLfDI wandte sich mit einem Auskunftersuchen an die Geschäftsführung der Therme. Der externe Datenschutzbeauftragte des Unternehmens antwortete und reichte die benötigten Nachweise ein. In der Therme war eine Videoüberwachungsanlage mit fünf Kameras installiert. Sie erfasste den Wert- und Kleiderspindbereich mit den dazwischenliegenden Gängen zum Zwecke der Prävention bzw. Aufklärung von Straftaten wie Schrankaufbrüchen und Vandalismus. Durch eine Videoüberwachung werden personenbezogene Daten erhoben, Aufnahmerekorder speichern diese und führen damit eine Verarbeitung der Daten durch. Gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet.

Vorliegend wurden keine schriftlichen Einverständniserklärungen der Besucher eingeholt, was bei einer unbestimmten Anzahl an Besuchern auch praktisch nicht umsetzbar ist. Ebenso wurden von den betroffenen Mitarbeitern keine Einwilligungserklärungen abgegeben. Allerdings wären letztere auch nur unter äußerst engen Voraussetzungen möglich. Dem Arbeitnehmer müssen Wahlmöglichkeiten gegeben werden, sodass er auch ohne Betreten des überwachten Bereichs seiner Arbeit nachkommen kann. Erst dann kann eine Freiwilligkeit bei der Einverständniserklärung angenommen werden. Im vorliegenden Fall mussten die Mitarbeiter, insbesondere das Reini-

gungspersonal, den videoüberwachten Bereich zwangsläufig betreten, um ihre Tätigkeit ausüben zu können.

Somit verbleibt zur Beurteilung der Zulässigkeit der Videoüberwachungsanlage nur noch § 6b BDSG. Diese Norm regelt die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Die Therme ist einem unbestimmten Personenkreis zugänglich, womit es sich um einen öffentlich zugänglichen Raum handelt.

Gem. § 6b Abs. 1. Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Hier soll die Videoüberwachungsanlage zur Gewährleistung der Prävention bzw. Aufklärung von Straftaten wie Schrankaufbrüchen und Vandalismus dienen. Solange eine tatsächliche Gefahrenlage nachgewiesen werden kann, ist darin grundsätzlich ein berechtigtes Interesse zu erkennen. Jedoch muss dieser Umstand mit konkreten Nachweisen aus der Vergangenheit belegt werden. Dies erfolgte nach erneutem Nachfragen. Jedoch muss die Videoüberwachung auch erforderlich sein.

Dafür muss die Kameraüberwachung zur Erreichung dieses Zwecks geeignet sein und kein milderes Mittel darf zur Verfügung stehen, um den angestrebten Zweck bei gleicher Effektivität zu erreichen. Für den festgelegten Zweck sind jedoch einige Alternativen ersichtlich. Zunächst könnte ein besseres Schlosssystem in die Spinde eingebaut werden oder das Badepersonal könnte Kontrollgänge durchführen. Auch möglich wäre das Bereitstellen von Wertschließfächern im Kassenbereich, sodass diese sich unter ständiger Kontrolle des Kassenpersonals befinden. Ebenso sind Anhaltspunkte ersichtlich, dass schutzwürdige Interessen von Betroffenen überwiegen. Dabei ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Eine Videoüberwachung im Umkleide- und Spindbereich stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar.

In diesem Bereich sind Menschen typischerweise spärlich bekleidet, und selbst wenn die Umkleidekabinen von dem Spindbereich getrennt sind, kann nicht automatisch davon ausgegangen werden, dass sich Besucher nicht doch in diesem Bereich entkleiden. Vor allem bei einem erhöhten Besucherandrang, wenn alle Umkleidekabinen belegt sind, werden manche Besucher den Spindbereich zum Umziehen nutzen. Eine Beobachtung der Intimsphäre durch eine Videoüberwachung stellt grundsätzlich keine verhältnismäßige und datenschutzrechtlich zulässige Maßnahme dar.

Somit überwiegen die schutzwürdigen Interessen der Besucher (Wahrung der Intimsphäre) gegenüber einer Überwachung zur Sicherung des Eigentums.

Der TLfDI ordnete das Entfernen der Kameras an. Dieser Aufforderung kam die verantwortliche Stelle auch nach. Das Verfahren konnte beim TLfDI daraufhin abgeschlossen werden. Die Einleitung eines Bußgeldverfahrens seitens des TLfDI gegen die verantwortliche Stelle wird derzeit geprüft.

Die Videoüberwachung im öffentlichen Bereich durch nicht-öffentliche Stellen ist nur in engen Grenzen zulässig. Der Gesetzgeber hat dies ausdrücklich und abschließend in § 6b BDSG geregelt. Gem. § 6b Abs. 1. Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.70 Wildtierkameras

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seitens einer Polizeibehörde, welche sich mit immer wiederkehrenden Anfragen von Bürgern auseinandersetzen musste, befragt, ob ein privater Jagdpächter im Wald Wildtierkameras an Bäumen anbringen kann. Zunächst ist darauf hinzuweisen, dass seit dem Urteil des *Verwaltungsgerichts Saarland vom 18. Mai 2016, Az.: 1 K 63/15* (siehe *Pressemitteilung des TLfDI vom 19. Mai 2017 Anlage 4*), welches durch Urteil des Oberverwaltungsgerichts Saarlouis vom

14. September 2017 bestätigt wurde, feststeht, dass auch Wildtierkameras der Meldepflicht des § 4d Abs. 1 BDSG unterliegen, da auch auf diese das Bundesdatenschutzgesetz anwendbar ist. Die Zulässigkeit des Einsatzes von Wildkameras durch nicht-öffentliche Stellen, wozu auch Privatpersonen (auch als Jäger) gehören, beurteilt sich nach § 6b Bundesdatenschutzgesetz (BDSG), da nach dem Thüringer Waldgesetz das Betreten des Waldes jedem gestattet ist und es sich somit um einen öffentlich zugänglichen Raum handelt. Nach § 6b Abs. 1 Nr. 3 BDSG ist der Betrieb von Wildkameras dann zulässig, wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse der Jäger ist anzunehmen, soweit die Verwendung der Kameras den Bestand und den Wechsel des Wildes im Jagdbezirk feststellen soll. Jedoch überwiegen die schutzwürdigen Interessen der Betroffenen (z. B. Spaziergänger, Sporttreibende, Pilz- und Kräutersammler), sich im Wald unbeobachtet von technisch elektronischen Einrichtungen aufzuhalten. Im Ergebnis hält der TLfDI den Einsatz von Wildkameras in öffentlich zugänglichen Waldgebieten regelmäßig für unzulässig. Ausnahmen ergeben sich für die Bereiche, die ausschließlich und erkennbar vom Jagdrevierinhaber betreten werden dürfen, oder dann, wenn die Kameras so aufgestellt sind, dass eine Beobachtung von Personen unwahrscheinlich ist, etwa in entlegenen Waldgebieten oder durch das Anbringen der Kameras in entsprechend niedriger Höhe. Zudem müssen in allen Fällen, in denen die Installation einer Wildkamera in einem öffentlich zugänglichen Raum datenschutzrechtlich zulässig ist, gemäß § 6b Abs. 2 BDSG der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar gemacht werden.

Das Betreiben von Wildtierkameras durch die private Jägerschaft unterfällt seit dem Urteil des Verwaltungsgerichts Saarland vom 18. Mai 2016, Az. 1 K 63/15 (Pressemitteilung des TLfDI vom 19. Mai 2016) der sog. Meldepflicht des § 4d Abs. 1 BDSG. Durch das Oberverwaltungsgericht des Saarlands wurde dieses Urteil am 14. September 2017 bestätigt. Das Anbringen von Wildtierkameras in öffentlich zugänglichen Waldgebieten ist regelmäßig unzulässig, jedoch bestehen Ausnahmen, wenn in entlegenen Waldgebieten oder

durch das Anbringen der Kameras in entsprechend niedriger Höhe kein Personenbezug hergestellt werden kann.

6.71 Spielhalle: Videogaga 27

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über eine Videoüberwachungsanlage in einer Spielhalle. Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Spielhallenbetreiber. Dieser teilte mit, dass die Videoüberwachungsanlage aus 16 Kameras bestehe, die folgende Bereiche erfasse:

Eingangsbereiche der Halle, beide Thekenbereiche, alle Geldspielgeräte sowie alle nicht von der Theke aus einsehbaren Bereiche. Die Aufnahmen werden elektronisch auf einer Festplatte für zehn Werktage gespeichert. Die Überwachung bestehe aufgrund der Unfallverhütungsverordnung (UVV) für Spielhallen, Spielcasinos und Automatenäle (§ 6 UVV), die sie verpflichtet, eine optische Raumüberwachung zu gewährleisten. Als Zweck der Überwachung wurden der Schutz des Personals, die Prävention und Abschreckung gegen potenzielle Straftäter und zum anderen die Erleichterung der Strafverfolgung angegeben. Die Mitarbeiter seien über die Videoüberwachung informiert worden und hätten alle mit einer schriftlichen Einverständniserklärung zugestimmt.

Nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung bedarf gem. § 4a BDSG der Schriftform. Vorliegend wurden keine schriftlichen Einverständniserklärungen von den Besuchern eingeholt, was bei einer unbestimmten Anzahl an Besuchern auch praktisch nicht umsetzbar ist. Zudem muss die Einwilligung vor der Datenerhebung erfolgen. Allerdings werden bereits mit Betreten der Spielhalle (Kamera im Eingangsbereich) Daten der Besucher erhoben.

Zwar wurde von den Mitarbeitern eine schriftliche Einwilligung abgegeben, jedoch ist eine solche Einwilligung nur unter äußerst engen Voraussetzungen möglich. Dem Arbeitnehmer müssen Wahlmöglichkeiten gegeben werden, sodass er auch ohne Betreten des überwachten Bereichs seiner Arbeit nachkommen kann. Erst dann kann eine Freiwilligkeit bei der Einverständniserklärung angenom-

men werden. Vorliegend war dies nicht möglich, da die Spielhalle flächendeckend überwacht wurde.

§ 6 Abs. 2 der Unfallverhütungsvorschrift für Spielhallen, Spielcasinos und Automatenäle von Spielbanken (UVV BGV C3) fordert, dass optische Raumüberwachungsanlagen so installiert sind, dass wesentliche Phasen eines Überfalles optisch wiedergegeben werden können. Da eine Einwilligung also nicht infrage kommt, bedarf es einer Rechtsgrundlage, die die Videoüberwachung erlaubt. Die UVV stellt jedoch keine Rechtsgrundlage i. S. d. § 4 BDSG dar. Vielmehr ist die Zulässigkeit der Videoüberwachungsanlage anhand des § 6b BDSG, welcher die Videoüberwachung in öffentlich zugänglichen Bereichen regelt, zu prüfen. Demnach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Vorliegend wurde die Videoüberwachung zum Schutz vor Straftaten installiert. Darin ist grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Jedoch ist es in bestimmten Fällen auch möglich, eine abstrakte Gefährdungslage anzunehmen, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die im Hinblick auf Vermögens- und Eigentumsdelikte potenziell besonders gefährdet sind. Diese potenzielle Gefährdung kann bei einer Spielhalle unterstellt werden.

Das Videoüberwachungssystem muss allerdings auch erforderlich, also zur Erreichung des festgelegten Zwecks vor allem geeignet sein. Es darf kein milderes Mittel zur Verfügung stehen, das weniger in die Rechte der Betroffenen eingreift, um den angestrebten Zweck bei gleicher Effektivität zu erreichen. Zudem dürfen keine schutzwürdigen Interessen der Betroffenen überwiegen.

Aufgrund dieser Beschränkungen sah der TLfDI einige Aufnahmebereiche kritisch. Der Zeitvertreib in Spielhallen und das Spielen von Glücksspielen zählt zur Freizeitbeschäftigung der Betroffenen. Das dem Freizeitbereich zuzurechnende Verhalten untersteht einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen. Im Normalfall überwiegt hier das schutzwürdige Interesse der Betroffenen gegenüber einer Überwachung. Deswegen ist eine Vi-

deoüberwachung nur in den Bereichen gerechtfertigt, in denen eine erhöhte Gefahr der Kriminalität besteht (z. B. Geldautomaten, die aufgebrochen oder manipuliert werden können). Gemäß § 3 Abs. 5 des Thüringer Spielhallengesetzes (ThürSpielhallenG) muss die Aufsicht des Spielhallenbetreibers von ihrem regelmäßigen Aufenthaltsort aus, auch unter Zuhilfenahme technischer Einrichtungen, alle Spielgeräte einsehen und Spieler beobachten können. Daher sind die Videokameras mit dem Aufnahmebereich der Geldspielgeräte zulässig. Die Videokameras, welche die Sitzgruppen und die Snookertische erfassen, sind jedoch nicht zulässig.

Auch bemängelte der TLfDI die Aufnahmen im Thekenbereich, wo sich Mitarbeiter dauerhaft aufhalten. Die Überwachung öffentlich zugänglicher Räume mit Publikumsverkehr, die gleichzeitig Arbeitsplätze erfasst, unterliegt strengen Anforderungen. Möglich ist eine Videoüberwachung insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Dabei ist allerdings zu beachten, dass der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich beschränkt wird und die Beschäftigten soweit wie möglich ausgeblendet werden (Schwärzung des Aufnahmebereiches).

Außerdem beanstandete der TLfDI die lange Speicherfrist von zehn Tagen. Gemäß § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Videoaufnahmen werden nicht mehr benötigt, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Es sollte prinzipiell möglich sein, innerhalb von ein bis zwei Tagen zu klären, ob die Sicherung des Materials notwendig ist. Folglich hat die Löschung grundsätzlich spätestens nach 48 Stunden zu erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist akzeptiert werden.

Hierzu führte die verantwortliche Stelle aus: Die Manipulation an Spielautomaten ist nur beim elektronischen Auslesen der Geräte erkennbar. Dieses Auslesen kann jedoch nur alle 10 bis 14 Tage erfolgen, da es sonst zu Problemen bei der Erklärung der Vergnügungssteuer kommt. Diese Einwände können aber nur bei Kameraaufnahmen berücksichtigt werden, die Geldspielgeräte überwachen. Bereits während des Schriftverkehrs demonstrierte die verantwortliche Stelle zwei Kameras, die vom TLfDI beanstandet wurden.

Da die Mitarbeiterüberwachung im Bereich der Theke und die lange Speicherung für alle Videokameras weiterhin vonstattengingen, erließ der TLfDI einen Anordnungsbescheid. In diesem gab er der verantwortlichen Stelle auf, die Kamera, die einen Snookertisch erfasste, innerhalb von zwei Wochen nach Bestandskraft des Bescheids zu entfernen. Außerdem soll die Speicherfrist aller Kameras, die keine Geldspielgeräte bewachen, auf 48 Stunden verkürzt werden. Weiterhin waren die Aufnahmebereiche der Kameras mit Blick auf die Thekenbereiche zu schwärzen, sodass die Mitarbeiter nicht mehr erkennbar waren. Wahlweise können die Kameras auch an einen Alarmknopf gekoppelt werden, sodass die Aufnahme erst durch eine Betätigung dieses Knopfes ausgelöst wird. Diesen Anforderungen kam die verantwortliche Stelle nach. Daraufhin konnte das Verwaltungsverfahren abgeschlossen werden.

Gem. § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In Fällen der Mitarbeiterüberwachung und Freizeitgestaltung der Betroffenen überwiegt zumeist das schutzwürdige Interesse des Betroffenen (Überwachten) gegenüber dem Interesse des Bewachers. Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, sobald feststeht, dass das Videomaterial nicht mehr benötigt wird. Grundsätzlich sollte nach 48 Stunden zu klären sein, ob eine Straftat vorgefallen ist. In begründeten Einzelfällen kann eine längere Speicherfrist akzeptiert werden.

6.72 Fahrgäste im Visier – Videogaga 28

Seit einigen Jahren steht der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nun schon in Kontakt mit einem öffentlichen Nahverkehrsbetrieb (3.10 Busfahrer im Visier Videogaga 3 TB 2012/13) wegen der Installation von Kameras in dessen Bussen. Nachdem dort bereits eine datenschutzrechtliche Kontrolle erfolgt war, ruhte das Verfahren zunächst, da eine Einigung der Datenschutzaufsichtsbehörden im Düsseldorfer Kreis zu dieser Problematik abgewartet werden sollte. Dort wurde eine „Ori-

entierungshilfe in öffentlichen Verkehrsmitteln“ erstellt, welche auf der Website des TLfDI https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh_v_pnv_sta_nd_09_2015_dk.pdf zum Abruf zur Verfügung steht. Aufgrund der am 25. Mai 2018 Geltung erlangenden Europäischen Datenschutz-Grundverordnung (DS-GVO) wird diese Orientierungshilfe an die rechtlichen Neuerungen im Zusammenhang mit Videoüberwachungen angepasst werden. Die aktualisierte Orientierungshilfe wird dann ebenfalls auf der Website des TLfDI abrufbar sein.



Das Verfahren wurde nach Erstellung der Orientierungshilfe wieder aufgegriffen. Der TLfDI wollte zunächst von dem Betrieb erfahren, ob seit der Kontrolle Änderungen in Bezug auf die Videoüberwachung erfolgt sind. In den 26 Bussen wurden weiterhin jeweils 4 Kameras betrieben, welche den gesamten Fahrgastraum überwachten. Zudem konnten durch die Kameras teilweise Außenaufnahmen gefertigt werden. Ferner war auch zum Teil der Fahrerbereich zu erkennen.

Die Videoaufnahmen wurden in den Bussen ohne Vorfall 72 Stunden gespeichert. Diese Aufnahmen konnten mittels Auslösen eines Notfallschalters im Rahmen eines Vorfalls durch den Busfahrer dauerhaft gespeichert werden. Aufgrund der Aufnahmen und der anschließenden Speicherung werden personenbezogene Daten erhoben und verarbeitet. Nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Weder eine gesetzliche Grundlage außerhalb des BDSG war für den TLfDI ersichtlich, noch kam eine Einwilligung für die Videoüberwachung in Betracht. Die Zulässigkeit der Videoüberwachung in den Bussen richtete sich nach § 6b BDSG, da es sich hierbei um öffentlich zugängliche Räume handelt, welche von jedermann betreten werden können. Nach § 6b Abs. 1 Nr. 2 und 3 BDSG ist eine Überwachung mit optisch-elektronischen Einrichtungen zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zudem ist mit dem seit dem

4. Mai 2017 in Kraft getretenen Videoüberwachungsverbesserungsgesetz der neue Satz 2 zu berücksichtigen, wonach bei der Videoüberwachung von Fahrzeugen des öffentlichen Busverkehrs der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse gilt. In den angeführten Zielen für die Videoüberwachung in der Datenschutzvereinbarung des Betriebes wurde u. a. angeführt: präventive Wirkung und Verringerung von strafbaren Handlungen wie z. B. Sachbeschädigungen, Eigentumsdelikte, Körperverletzungen und gefährliche Eingriffe in den Busverkehr sowie die verbesserte Strafverfolgung dieser einzelnen Delikte. Da vorliegend der Schutz von Leben und Gesundheit ein vordergründiges Ziel des Unternehmens zum Betreiben der Videoüberwachung war, musste dies bei den berechtigten Interessen und im Rahmen der Interessenabwägung berücksichtigt werden. Zudem war seitens des Unternehmens eine konkrete Gefahrenlage nachzuweisen, was durch die Nennung entsprechender Vorkommnisse mit den polizeilichen Tagebuchnummern ohne Probleme erfolgte. Ferner musste die Videoüberwachung für den festgelegten Zweck geeignet und erforderlich sein. Im Rahmen der Erforderlichkeitsprüfung ist nicht nur das „Ob“ der Videoüberwachung zu überprüfen, sondern auch das „Wie“. Dabei ist insbesondere der räumliche und zeitliche Umfang der Überwachung zu berücksichtigen. Vorliegend bestanden Bedenken hinsichtlich der durchgehenden Speicherung, obwohl es möglich war, mittels Notfallschalter im Rahmen eines Vorkommnisses die Aufnahme auszulösen. Zudem bestanden datenschutzrechtliche Bedenken betreffend der Außenaufnahmen durch die Videokameras. Hier waren auf den einzelnen Screenshots parkende Pkw zu erkennen, wenn auch nicht mit deren Kennzeichen, sowie die an den Haltestellen wartenden Personen. Eine Schwärzung der Aufnahmen war technisch nachweisbar nicht möglich, jedoch ist die Ausrichtung der Kameras so vorzunehmen, dass entweder keine Außenaufnahmen oder nur solche ohne Personenbezug stattfinden. Diese sind für die von dem Unternehmen genannten Zwecke nämlich nicht erforderlich. Zudem bestanden vorliegend Anhaltspunkte, dass schutzwürdige Interessen der betroffenen Fahrgäste überwiegen. Entscheidend ist hierbei die Eingriffintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes) durch den betroffenen Per-

sonenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt. Das Unternehmen überwachte vorliegend während der gesamten Fahrtzeit auf jeder Linie den kompletten Fahrgastraum. Das informationelle Selbstbestimmungsrecht der Fahrgäste in diesen Bereichen ist besonders intensiv betroffen, da Menschen dort typischerweise miteinander kommunizieren, sich aber jedenfalls längere Zeit aufhalten. Hinzu tritt, dass die Fahrgäste häufig auf die Nutzung der öffentlichen Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel und damit der Videoüberwachung ausweichen können. Ferner ist dort eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine Beobachtung geben. Ein solch intensiver Eingriff in das Recht auf informationelle Selbstbestimmung ist nur zum Schutz von Rechtsgütern erheblichen Gewichts (z. B. Schutz vor Gewalt von Personen) gerechtfertigt. Mit dem Urteil des Obergerichts Niedersachsen vom 07.09.2017, Az.: 11 LC 59/16 ergaben sich erhebliche Änderungen bei der Beurteilung der Zulässigkeit von Videoüberwachungen im Personennahverkehr. Eine Differenzierung des Einsatzes der Videoüberwachung nach Strecken, Tageszeiten und Fahrzeugbereichen, wie bisher durch die Aufsichtsbehörden gefordert, wurde seitens des Gerichts abgelehnt, da das Unternehmen vortragen konnte, dass Störungen und Vorkommnisse auf sämtlichen Strecken und zu jeder Tag- und Nachtzeit vorgefallen sind. Auch bei dem hier geprüften Busunternehmen konnte dieser Sachverhalt festgestellt werden. Jedoch wurde durch das Gericht auch in der Interessenabwägung berücksichtigt, dass bestimmte technische organisatorische Maßnahmen seitens der Unternehmen zu treffen sind, um dadurch die schutzwürdigen Interessen der Betroffenen umfassend zu berücksichtigen. Insbesondere sind hier zu nennen: eine kurze Speicherfrist (24 Stunden), bei der Auswertung der Datenträger müssen Zugriffsbeschränkungen bestehen, die Daten müssen in einem gesonderten abschließbaren Raum gesichert werden zu dem nur ein schriftlich festgelegter Personenkreis Zugriff hat und diese Daten dürfen nur auf einen nicht vernetzten Computer abgelegt werden. Der TLfDI schloss sich im vorliegenden Fall der Auffassung des Obergerichts an. Dem Unternehmen wurde die geänderte Rechtsauffassung mitgeteilt. Jedoch sind weiterhin die Außenaufnahmen aus den Bussen heraus unzulässig. Auch sind seitens des Unternehmens entsprechende technische organisatorische Maßnahmen, wie in dem Urteil aufgeführt, zu treffen und schriftlich festzulegen. Das Verfah-

ren ist beim TLfDI daher noch nicht abgeschlossen. Über den Ausgang des Verfahrens wird voraussichtlich in dem nächsten Tätigkeitsbericht abschließend informiert werden.



Bisher wurde seitens der Aufsichtsbehörden bei der Videoüberwachung in öffentlichen Verkehrsmitteln von den verantwortlichen Stellen eine Differenzierung der Überwachung gefordert. Die entsprechende Orientierungshilfe zur Videoüberwachung in öffentlichen Verkehrsmitteln wird auf der Website des TLfDI bereitgestellt (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh_v_pnv_st_and_09_2015_dk.pdf). Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereiches nach § 6b BDSG ist danach unverhältnismäßig und daher unzulässig. Die Erwägungen des Urteils des Oberverwaltungsgerichts Niedersachsen, sowie das Videoüberwachungsverbesserungsgesetz führen jedoch aus Sicht des TLfDI dazu, dass eine Videoüberwachung in Bussen und sonstigem öffentlichen Verkehr zukünftig eher als zulässig zu betrachten sein wird. Jedoch verbleibt es dabei, dass jede eingesetzte Videoüberwachung auch im Personennahverkehr eine Einzelfallentscheidung bleibt und keine generelle Zulässigkeit von Videoüberwachungen in Bussen und Bahnen angenommen werden kann.

6.73 Kameras im Imbiss – Videogaga 29

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde aufgrund einer Beschwerde eine Videoüberwachung in einem Imbiss bekannt. Der TLfDI ermittelte zunächst die Eigentümer des Imbisses und wandte sich mit einem Auskunftersuchen an die Inhaber. Diese teilten mit, dass zwei Videokameras installiert wurden. Die erste Kamera war auf den Eingangsbereich gerichtet, welche jedoch auch den Bereich der Stehti-

sche erfasste. Eine weitere war auf die Kasse ausgerichtet. Diese Kamera wurde jedoch nur eingeschaltet, wenn die Betreiber des Imbisses allein im Geschäft waren und einer von beiden in den Keller gehen musste. Die Kamerabilder wurden dann auf einen kleinen Monitor übertragen, um die Kasse im Blick zu behalten. Es erfolgte keine Aufzeichnung, sondern eine Echt-Zeit-Beobachtung (Monitoring) mittels der Kameras.

Maßgebliche Vorschrift für die Beurteilung der Zulässigkeit der hier betriebenen Videokameras ist § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG), da es sich bei dem Gastraum während der Öffnungszeiten um einen öffentlich zugänglichen Raum handelt. Danach ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Problematisch war hier insbesondere die Kamera, welche auf den Stehtischbereich ausgerichtet war. Die Videoüberwachung des Gastraums einer Gaststätte ist nach § 6b BDSG im Regelfall datenschutzrechtlich unzulässig. Gemeint ist die Gaststätte i. S. d. § 1 Gaststättengesetzes (GastG), d. h. ein Betrieb, in welchem Getränke und/oder Speisen zum Verzehr an Ort und Stelle verabreicht werden und der jedermann oder bestimmten Personenkreisen zugänglich ist. Darunter fallen insofern auch Imbisslokale und Schnellrestaurants. Die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind die Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und somit nicht mit Videokameras überwacht werden dürfen (siehe hierzu Urteil des Amtsgerichts Hamburg vom 22. April 2008 – 4 C 134/08). Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechnigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann. Im vorliegenden Fall wurde seitens der Imbissinhaber auch kein berechtigtes Interesse zum Betreiben der Kamera benannt, sodass in jedem Fall die schutzwürdigen Interessen über-

wiegen. Hinsichtlich der anderen Kamera, welche auf die Kasse ausgerichtet war, bestanden keine Bedenken, da diese nur für den Fall eingeschaltet wurde, dass die Betreiber allein im Lokal waren und Mitarbeiter- sowie Kundeninteressen nicht betroffen waren.

Der TLfDI teilte den Betreibern der Videokameras seine Rechtsauffassung mit, woraufhin diese die problematische Kamera deinstallierten. Ein weiteres Einschreiten des TLfDI war daher nicht erforderlich.

Im Berichtszeitraum wurde der TLfDI mehrmals auf Videoüberwachungen in Gasträumen von Gaststätten aufmerksam gemacht. Die Videoüberwachung von Gasträumen, welche mit Tischen und Sitzgelegenheiten ausgestattet sind, ist während der üblichen Geschäftszeiten oder wenn sich sonstiges Personal darin aufhält, im Regelfall datenschutzrechtlich aufgrund des intensiven Eingriffs in das informationelle Selbstbestimmungsrecht der Gäste oder des Personals unzulässig. Gerade in diesem Freizeitbereich, wo die ungestörte und unbeeinträchtigte Kommunikation im Vordergrund steht, ist der Schutz der Betroffenen vor Beobachtung in diesem Bereich besonders wichtig.

6.74 Mieter unter Beobachtung – Videogaga 30

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde seitens eines Bürgers auf eine Videoüberwachung aufmerksam gemacht, welche auf die öffentliche Straße und den Gehweg gerichtet war. Im Wege der Amtshilfe durch eine thüringische Stadtverwaltung konnte tatsächlich eine Kamera an der Einfahrt zum Hinterhof festgestellt werden. Gleichzeitig wurde der Eigentümer des Gebäudes hinsichtlich der betriebenen Videoüberwachung mittels Auskunftersuchens angeschrieben, um den Sachverhalt zu ermitteln.

Der Eigentümer teilte daraufhin mit, dass er zwei Videokameras an dem Gebäude installiert hatte. Eine Kamera war an der Toreinfahrt angebracht und so ausgerichtet, dass sie den Eingang zum Haus, sowie die Briefkästen und den Fahrradständer erfasste. Der Gehweg und die öffentliche Straße wurden ausgepixelt und waren nicht zu erkennen. Eine weitere Kamera befand sich im hinteren Hausbereich, welche ebenfalls den Fahrradständer und den Sitz- und Bankbereich im Garten abbildete. Das Gebäude bewohnte zum einen der Eigen-

tümer selbst, zum anderen lebten dort mehrere Mietparteien. Als Zweck zum Betreiben der Kameras gab der Eigentümer an, dass die Abschreckung von Vorfällen wie das Stehlen von Fahrrädern, Graffitiverschmutzungen und Beschädigungen am Fahrzeug im Vordergrund steht.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar wurde seitens des Eigentümers eine Liste von Einwilligungserklärungen seitens der Mieter eingereicht, jedoch wurde die Einwilligung entgegen § 4a Abs. 1 BDSG erst nach Datenerhebung erteilt und war daher nicht mehr zu berücksichtigen. Hinzu kommt, dass auch die Besucher, sowie sonstige von der Videoüberwachung Betroffene vor der Erhebung der personenbezogenen Daten, also vor Betreten des videoüberwachten Bereichs eine schriftliche Einwilligung erteilen müssten, was praktisch nicht umsetzbar ist. Daher scheidet eine Einwilligung für die in diesem Fall betriebene Videoüberwachung aus.

Bei den beiden Kameras ist zu unterscheiden, welche Bereiche durch die Aufnahmen erfasst werden. Bei der Kamera, welche den Eingangsbereich überwacht, beurteilt sich die Zulässigkeit der betriebenen Videoüberwachung nach § 6b Abs. 1, 3 BDSG. Danach ist eine Beobachtung mittels optisch-elektronischen Einrichtungen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung des berechtigten Interesses für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei dem mit der ersten Kamera überwachten Hauseingangsbereich handelt es sich um die Überwachung eines öffentlich zugänglichen Raums, da dieser von jedermann betreten werden kann. Der von dem Betreiber genannte Zweck kann dann ein berechtigtes Interesse zum Betreiben der Videoüberwachung darstellen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Hierfür trug der Eigentümer im weiteren Verfahren vor, dass es in der Vergangenheit zu Strafanzeigen wegen Fahrraddiebstählen, Sachbeschädigungen an der Gebäudewand und am privaten Pkw gekommen sei. Die Aufzählung der Vorkommnisse reichte in diesem Fall aus, um ein berechtigtes Interesse bejahen zu können.

Es bestanden jedoch Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen, in diesem Fall der Mieter und der Besucher des Hauses, die berechtigten Interessen am Betreiben der Videoüberwachung überwiegen. Die dauerhafte Überwachung von Eingängen zu Wohngebäuden lässt Rückschlüsse auf den Tagesablauf und die sonstige Lebensführung der Mieter zu. Die Bilder dokumentieren einen nicht unerheblichen Bereich des Privatlebens. Auch werden Besucher der Mieter miterfasst. Hinzu kommt, dass die Mieter und Besucher des Gebäudes auf die Nutzung des Eingangs angewiesen sind, sodass hier ein erheblicher Eingriff in deren informationelles Selbstbestimmungsrecht vorliegt. Eine Überwachung in diesem Bereich kann nur dann zulässig sein, wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers nicht in zumutbarer anderer Weise begegnet werden könnte (LG Berlin, Urteil vom 23. Mai 2005, Az. 62 S 37/05). Hierzu wurde seitens des Betreibers nichts vorgetragen. Die genannten Vorkommnisse waren nicht so schwerwiegend, dass eine Videoüberwachung in diesem Bereich gerechtfertigt wäre.

Die zweite Kamera war in einem nicht-öffentlich zugänglichen Bereich angebracht, da hier nur die Bewohner und Eigentümer des Hauses Zutritt zum Hinterhof und Gartenbereich hatten. Hier richtet sich die Beurteilung der Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen an dem Ausschluss der Verarbeitung überwiegen. Hier gelten ähnliche Voraussetzungen für eine Videoüberwachung wie bei § 6b BDSG, sodass insbesondere auf die oben gemachten Ausführungen zum berechtigten Interesse verwiesen wird. Vorliegend bestanden bei der Kamera Bedenken hinsichtlich der Erforderlichkeit. Ausreichend für den genannten Zweck war eine Ausrichtung nur auf den Fahrradständer. Zudem gab es Anhaltspunkte für das Überwiegen schutzwürdiger Interessen von Betroffenen, also den Mietern des Hauses. Da der Sitzbereich, als Ruhe- und Kommunikationsmöglichkeit der freien Entfaltung der Persönlichkeit dient, stellt eine dauerhafte Überwachung einen erheblichen Eingriff in das Freizeitverhalten der Nutzer dieses Bereichs dar. Beide Kameras sah der TLfDI im Hinblick auf die Ausrichtung für unzulässig an. Diese Auffassung wurde dem Eigentümer mitgeteilt.

Das Verfahren ist noch nicht abgeschlossen, da eine weitere Verpixelung der nunmehr eingereichten Videobilder erfolgen muss.

Bei der Videoüberwachung von Hauseingangsbereichen handelt es sich um die Überwachung von öffentlich zugänglichen Räumen, unabhängig davon, ob sich diese auf dem eigenen Grundstück befinden. Insbesondere in Mehrfamilienhäusern mit Mietparteien ist dieser Bereich als datenschutzrechtlich sehr empfindlich einzustufen. Hier überwiegen die schutzwürdigen Interessen der Betroffenen zumeist die berechtigten Interessen der Betreiber der Videoüberwachung. Die Mieter und deren Besucher sind auf die Nutzung des überwachten Bereichs angewiesen. Die Form der Überwachung lässt zudem Rückschlüsse auf deren Tagesablauf und die sonstige Lebensführung zu und liefert neben der hohen Informationsdichte einen besonderen Informationsgehalt. Dabei dokumentieren die Bilder einen nicht unerheblichen Bereich des Privatlebens. Eine Überwachung in diesem Bereich kann nur dann zulässig sein, wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers nicht in zumutbarer anderer Weise begegnet werden könnte (LG Berlin, Urteil vom 23. Mai 2005, Az. 62 S 37/05).

6.75 Videokameras als Türsteherersatz? – Videogaga 31

Im Berichtszeitraum hat eine Stadtverwaltung dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Videoüberwachung im Außenbereich einer Diskothek gemeldet, welche auch die öffentliche Straße und Gehwege miterfassen sollte. Der TLfDI wandte sich daraufhin an die Betreiber der Diskothek, um mithilfe eines Auskunftersuchens den Sachverhalt aufzuklären.

Der Diskothekenbetreiber teilte mit, dass vier Videokameras installiert waren. Eine Kamera befand sich im inneren Eingangsbereich der Diskothek, zwei waren außen seitlich zum Eingang gerichtet angebracht. Diese bildeten die Straßenkreuzung sowie einen Großteil des Gehweges mit ab. Eine weitere Kamera war an der Eingangstür Richtung Straße ausgerichtet. Die Kameras zeichneten nicht auf und wurden während der Öffnungszeiten der Diskothek eingeschaltet. Die Kameras sollten zur Gefahrenabwehr eingesetzt werden.

Die Zulässigkeit der betriebenen Videoüberwachung richtet sich während der Öffnungszeiten vorliegend nach § 6b Abs. 1 Bundesda-

tenschutzgesetz (BDSG), wonach das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Der angegebene Zweck Gefahrenabwehr war im vorliegenden Fall zu unkonkret, da nicht deutlich wurde, welche Gefahren genau abgewehrt werden sollten. Hierzu ist es auch erforderlich, eine tatsächliche Gefahrenlage nachzuweisen, d. h. etwaige Vorkommnisse aus der Vergangenheit mit Datum, Art und Schadenshöhe zu dokumentieren oder polizeiliche Tagebuchnummern oder staatsanwaltschaftliche Aktenzeichen zu nennen. Im Verwaltungsverfahren hatte der Betreiber der Videoüberwachung hierzu nichts vorgetragen. Insofern lag kein berechtigtes Interesse zum Betreiben der Videokameras vor. Zudem bestanden Bedenken hinsichtlich der Erforderlichkeit der Videoüberwachungsanlage. Es darf kein gleich geeignetes milderes Mittel zum Erreichen des Zwecks vorhanden sein. Es wäre möglich, entsprechendes Sicherheitspersonal während des Einlasses zu positionieren, um ein Eingreifen bei entsprechenden Delikten vor der Tür zu ermöglichen. Dies ist eine gängige Praxis bei Diskotheken. Aber nicht nur das „Ob“ des Einsatzes der Videoüberwachung ist Gegenstand der Erforderlichkeitsprüfung, sondern auch das „Wie“, also der zeitliche und räumliche Umfang der eingesetzten Videotechnik. Insbesondere die Kameras im Außenbereich, welche die öffentliche Straße und einen Großteil des Gehwegs überwachten, waren für den Zweck nicht erforderlich. Die Kameras waren hier so auszurichten, dass die Straße außerhalb des Erfassungsbereichs lag. Da kein berechtigtes Interesse zum Betreiben der Kameras bejaht werden konnte, musste die Erforderlichkeit im Rahmen der Wahrnehmung des eigenen Hausrechts überprüft werden. Die Ausrichtung ist hier lediglich bis einen Meter von der Hauswand entfernt in den öffentlichen Raum zulässig, was in diesem Fall ebenfalls nicht erfüllt war. Der TLfDI teilte dem Betreiber der Videokameras seine Rechtsauffassung mit. Der Diskothekenbetreiber stellte daraufhin die komplette Videoüberwachung in seiner Diskothek ein, sodass ein weiteres Einschreiten des TLfDI nicht erforderlich war.

Der Einsatz einer Videoüberwachung sollte seitens der verantwortlichen Stelle genau überlegt werden. Insbesondere die mit der Videoüberwachung verfolgten Zwecke sind so konkret wie möglich zu

bezeichnen. Eine pauschale Angabe von Sicherheitsgründen oder zur Gefahrenabwehr reicht hierfür nicht aus. Die Erforderlichkeit jeder einzelnen Kamera ist an dem genannten Zweck zu überprüfen. Es scheitert hier sehr oft bereits an der Geeignetheit der Kamera zu diesem Zweck. Auch existieren oft mildere Mittel, deren Einsatz die verantwortlichen Stellen aufgrund des höheren Aufwandes scheuen.



Personal - ©Wolfilser / Fotolia.com

7 Beschäftigtendatenschutz

7.1 Videoüberwachung im Freizeitpark

Ein Besucher eines Freizeitparks nahm neben den dargebotenen Attraktionen auch immer wieder Videokameras wahr, während er vergeblich den vorgeschriebenen Hinweis darauf suchte. Er wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Datenschutzaufsichtsbehörde nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG), der nach § 38 Abs. 1 BDSG die Einhaltung datenschutzrechtlicher Bestimmungen kontrolliert, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Auf das an den Freizeitpark betreibende Unternehmen gerichtete Auskunftersuchen nach § 38 BDSG teilte dieses mit, es habe bereits vor Jahren 13 Kameras installiert, um den reibungslosen Betriebsablauf zu gewährleisten. Aufzeichnungen würden nicht angefertigt, es erfolge eine reine Beobachtung der erfassten Bereiche.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahr-

nehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Um die Zulässigkeit der Videoüberwachung prüfen zu können, wurde das Unternehmen gebeten, zu jeder einzelnen Kamera die Angabe des Zwecks der Videoüberwachung darzulegen. Es ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG. Weiterhin wurde erfragt, ob die verfolgten Zwecke tatsächlich mit der Videoüberwachung erreicht werden können. Ferner wurde das Unternehmen darauf hingewiesen, nach § 6b Abs. 2 BDSG den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mit Hilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

Gegen die Mehrzahl der Kameras bestanden keine datenschutzrechtlichen Bedenken. Sie beobachteten lediglich den Besucherstrom und ermöglichten dem Personal so, den Eintritt zu bestimmten Bereichen zu steuern. So wurde verhindert, dass sich zu viele Personen dort aufhielten. Problematisch war, dass neben den dargebotenen Attraktionen im Freizeitpark auch der Eingangsbereich mit Kassenhäuschen, das Restaurant im Innenbereich und der Andenken-Verkaufsraum überwacht wurden. Dies schloss eine Erfassung der Mitarbeiter in diesen Bereichen ein und konnte eine unzulässige Leistungs- und Verhaltenskontrolle ermöglichen. Daher kam der Abwägung mit den Interessen der Betroffenen im Sinne von § 6b

Abs. 1 BDSG besondere Bedeutung zu. Als zulässig sah der TLfDI an, den Zugang des Besucherstroms an den Kassenhäuschen gegebenenfalls zu koordinieren, wobei allerdings ausgeschlossen sein musste, dass der dort tätige Mitarbeiter einer ständigen Beobachtung ausgesetzt war. Andererseits konnte die Beobachtung der Gäste und Mitarbeiter im Restaurant nicht mit der Sicherstellung eines geordneten Betriebsablaufs begründet werden. Sollte dort weiteres Personal erforderlich sein, um das hohe Besucheraufkommen bewältigen zu können, kann man dies auf andere Weise, wie etwa eine telefonische Anforderung weiteren Personals, bewerkstelligen. Eine ständige Beobachtung des Bedienpersonals und der sich dort aufhaltenden Gäste war nicht erforderlich. Im Verkaufsraum musste ebenfalls nicht das Personal beobachtet werden. Ob letztendlich Diebstähle durch Besucher dort durch eine Beobachtung per Videokamera verhindert oder aufgeklärt werden konnten, erschien mehr als fraglich. Um im Falle eines vom Verkaufspersonal bemerkten Diebstahls oder gar Überfalls Hilfe anzufordern, hätte auch ein Notrufknopf ausreichen können. Daraufhin stellte das Unternehmen klar, dass es alle Kameras in eine Wechselschleife eingebunden hatte, sodass nur noch Einzelbilder in bestimmten Zeitabständen auf den Monitoren erschienen. Diese Einzelbilder seien aber unverzichtbar, um mit wenig Personal die komplexen Betriebsabläufe sicherzustellen. Im Übrigen habe man die Kameras im Restaurant so ausgerichtet, dass das Essverhalten der Besucher nicht mehr beobachtet werden konnte. Weiterhin hatte man Hinweisschilder angebracht, die auf die Kameraüberwachung aufmerksam machten. Daher war kein weiteres Vorgehen erforderlich.

Werden öffentlich zugängliche Räume mittels einer Videoanlage überwacht, ist der konkrete Zweck für jede einzelne Kamera vorab schriftlich festzulegen. Die Videobeobachtung muss für den angegebenen Zweck geeignet sein. Weiterhin muss mit den schutzwürdigen Interessen der von der Überwachung Betroffenen abgewogen werden. Eine ständige Beobachtung von Beschäftigten ist grundsätzlich nicht zulässig.

7.2 Frau am Facebook-Pranger

Eine Beschwerde einer zwischenzeitlich ausgeschiedenen Mitarbeiterin eines Unternehmens erreichte den Thüringer Landesbeauftrag-

ten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Arbeitnehmerin musste feststellen, dass ihr ehemaliger Arbeitgeber über das soziale Netzwerk „Facebook“ alle Welt wissen ließ, er habe gegen sie wegen Verdachts des gewerbs- und bandenmäßigen Betrugs in mindestens 50 Fällen Strafanzeige erstattet. Sie solle sich durch Verbuchung von Scheinlieferungen persönlich bereichert und einen Schaden in sechsstelliger Höhe verursacht haben.

Eine entsprechende Schadensersatzklage gegen die Mitarbeiterin war vom zuständigen Arbeitsgericht abgewiesen worden. Angefragt erklärte das Unternehmen, man sei gegen das Urteil in Berufung gegangen, aber von der Schuld der Betroffenen überzeugt. Weil eine gütliche Einigung nicht möglich war, habe man sich unter Inanspruchnahme des Grundrechts auf Meinungsfreiheit zu der Veröffentlichung auf der vorrangig firmeninternen Plattform entschlossen. Das sei man im Übrigen auch den anderen Mitarbeitern schuldig gewesen, denn der Vorgang habe innerhalb der Belegschaft für Unruhe gesorgt. Man habe ja auch nur von einem „Verdacht“ gesprochen.

Dass die Veröffentlichung auf <https://www.facebook.com> zweifellos nicht nur auf einer firmeninternen, sondern einer weltweit öffentlich zugänglichen Plattform erfolgt, hätte dem Unternehmen klar sein müssen. Verkannt wurde darüber hinaus auch, dass das Grundrecht auf Meinungsfreiheit seine Schranken in den Vorschriften der allgemeinen Gesetze findet und dass eine solche Schranke auch § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) darstellt. Danach ist eine Veröffentlichung personenbezogener Daten nur erlaubt, wenn dies eine Rechtsvorschrift zulässt oder die Einwilligung des Betroffenen vorliegt. Beides war in keiner Weise ersichtlich. Dass es sich bei der unzulässigen Veröffentlichung auf Facebook nicht um eine Lappalie handelt, zeigt schon, dass dies mit einem Bußgeld bis zu dreihunderttausend Euro geahndet werden kann (§ 43 Abs. 2 Nr. 1 und 2, Abs. 3 Satz 1 2. Halbsatz BDSG). Der TLfDI leitete daher auch ein Bußgeldverfahren ein.

Immerhin hatte das Unternehmen den Facebook-Eintrag nach kurzer Zeit gelöscht. Der weiteren Forderung, schriftliche Festlegungen durch das Unternehmen zur Nutzung von Facebook zu treffen, kam das Unternehmen letztendlich auf massives Drängen des TLfDI



nach. Danach dürfen grundsätzlich keine personenbezogenen Daten Beschäftigter auf dieser Plattform veröffentlicht werden, sofern keine wirksame Einwilligung der Betroffenen vorliegt. Wirksam ist eine Einwilligung allerdings nur, wenn sie freiwillig erteilt wurde. Im Beschäftigtenverhältnis ist dies nur dann der Fall, wenn der Beschäftigte unter keinerlei Zwang steht. Da man im Beschäftigtenverhältnis aber fast immer von einem gewissen Druck ausgehen kann, unter dem die Betroffenen stehen, die „gewünschte“ Einwilligung abzugeben, ist nur in sehr seltenen Fällen von Freiwilligkeit auszugehen. Festgelegt wurden auch die Verantwortlichkeiten für die Veröffentlichung und Modalitäten der Überwachung der Einträge.

Egal wie ärgerlich es ist, wenn man zu seinem vermeintlichen Recht nicht kommt. Eine Rechtfertigung, einen ehemaligen Mitarbeiter in sozialen Medien anzuprangern, gibt es nicht. Zum Betrieb von Facebook-Fanpages für Unternehmenszwecke sind entsprechende Festlegungen zu treffen.

7.3 (K)ein Kraftaufwand: Videoüberwachung im Fitnessstudio

Ein Bürger informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in einem Fitnessstudio im Eingangs- und Bürobereich Kameras installiert seien, um die Mitarbeiter hinsichtlich Verhalten, Tätigkeit und Leistung zu überwachen. Der Beschwerdeführer bat den TLfDI um datenschutzrechtliche Bewertung dieses Sachverhalts.

Für die Erstellung von Videoaufnahmen ist gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) eine gesetzliche Ermächtigung oder die Einwilligung des Betroffenen erforderlich. Als zuständige Aufsichtsbehörde kontrolliert der TLfDI gemäß § 38 Abs. 1 BDSG, ob bzw. dass Videoaufzeichnungen nach den datenschutzrechtlichen Bestimmungen erfolgen.

Auf Nachfrage teilte der Inhaber des Fitnessstudios dem TLfDI mit, dass er seit mehr als 2 Jahren eine Videoüberwachungsanlage mit zwei Kameras betreibe – eine im Eingangsbereich des Studios und eine im Büro. Der Inhaber legte dar, dass die Versicherung Schutzmaßnahmen gefordert hatte, nachdem zuvor wiederholt in das Fitnessstudio eingebrochen worden war. Andernfalls habe die Versicherung über eine Vertragskündigung nachdenken wollen. Daher habe

sich der Inhaber verpflichtet gesehen, das Fitnessstudio besser zu sichern.

Weiterhin gab der Inhaber an, dass die Kameraaufzeichnungen an einem sicheren Ort erfolgten und nicht während der Geschäftszeit angeschaut werden könnten. Die Daten würden acht Tage gespeichert, die Festplatte sei passwortgeschützt und müsse zur Einsichtnahme abgebaut und an einen Monitor angeschlossen werden. Zugriff hätten nur die Inhaber des Fitnessstudios, die Aufnahmen würden nicht an Dritte weitergegeben. Im Eingangsbereich des Studios, am Nebenausgang und an den Parkplätzen seien außerdem Hinweisschilder zu den Kameras angebracht. Einen Datenschutzbeauftragten gab es nach Angabe der Inhaber im Fitnessstudio nicht.

Nachdem der TLfDI um ergänzende Angaben zu den genauen Kameraeinstellungen und deren technischen Nutzung gebeten hatte, teilte der Inhaber des Fitnessstudios mit, dass er aufgrund der zeitaufwendigen Stellungnahmen die Videokameras abschalte. Der TLfDI forderte die Löschung der gesamten Videoaufnahmen und behielt sich eine Vor-Ort-Kontrolle vor.

Nach § 4 Abs. 1 BDSG bedarf die Erhebung von Videoaufnahmen einer gesetzlichen Ermächtigung oder persönlichen Einwilligung der bzw. des Betroffenen. Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Er kontrolliert nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Einhaltung entsprechender datenschutzrechtlicher Bestimmungen.

7.4 Mit GPS immer ein Auge auf die Mitarbeiter?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bekam einen anonymen Hinweis darauf, dass ein Dienstleistungsunternehmen sämtliche Fahrzeuge des Fuhrparks mit GPS-Systemen ausgerüstet habe. Die Mitarbeiter befürchteten, über die Nutzung ihrer Dienstfahrzeuge rund um die Uhr überwacht zu werden. Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Unternehmer und bat um nähere Informationen zur Ausstattung der Firmenwagen mit dem GPS-System, insbesondere zu den schriftlichen Festlegungen, der Speicherdauer und um Angabe des Zwecks der Datenverarbeitung.

Das Unternehmen, das einen externen Datenschutzbeauftragten bestellt hatte, teilte mit, man habe das GPS-System zunächst testweise erprobt und nutze es aktiv erst seit wenigen Tagen. Mit einem Informationsblatt war den Mitarbeitern zur Testphase nur die Tatsache des Einbaus von GPS-Technik zum Zweck der Schutzfunktion vor Diebstahl der Fahrzeuge mit teurer Messtechnik, zu Zwecken der Abrechnung mit Kunden und zur Optimierung des Einsatzes und der Tourenplanung zur Kenntnis gegeben worden. Gegen die Nutzung von GPS für diese Zwecke bestehen grundsätzlich keine datenschutzrechtlichen Bedenken, denn sie dienen der Wahrung berechtigter Interessen des Arbeitgebers nach § 28 Abs. 1 Nr. 2 BDSG, wobei das Interesse des Betroffenen in diesem Zusammenhang nicht überwiegt. Aus der Information ließ sich jedoch für die Betroffenen in keiner Weise ableiten, ob eine auf sie bezogene Auswertung oder eine Nutzung der erfassten Daten auch für arbeitsrechtliche Zwecke erfolgen sollte. In der zwischenzeitlich durch die Geschäftsleitung erstellten und mit dem Aktiveinsatz des GPS-Systems geltenden „Anweisung zur Nutzung GPS“ wurden die erforderlichen Festlegungen für die Verarbeitung der personenbezogenen Daten der Beschäftigten getroffen. Danach gelten geeignete Maßnahmen zum Schutz der Beschäftigten und namentlich restriktive Zugriffsbeschränkungen. Die Daten werden nach Erreichung der Zwecke, insbesondere die Abrechnung mit den Kunden, gelöscht. Es wurde festgelegt, dass eine permanente oder allgemeine Leistungs- und Verhaltenskontrolle nicht durchgeführt wird. Das System darf auch nicht in Fahrzeuge eingebaut werden, bei denen eine Privatnutzung für die Mitarbeiter zugelassen ist. Darüber hinaus erhalten die Mitarbeiter die Hinweise, um dem Gebot der Transparenz für die Betroffenen Rechnung zu tragen. Nachzulesen sind die Vorgaben auch unter den Hinweisen des LfD NRW https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/4_Ortungssysteme_und_Beschaeftigtendatenschutz/Ortungssysteme.pdf „Einsatz von Ortungssystemen und Beschäftigtendatenschutz“.

Nicht zu bemängeln war, dass auch Stichproben sowie bei begründetem Verdacht auf Pflichtverletzungen weitere Kontrollen vorgesehen werden. Dabei war vorgesehen, dass



der betriebliche Datenschutzbeauftragte nur jährlich hierüber informiert wird. Der TLfDI hielt es in diesem Zusammenhang jedoch für angebracht, den Beauftragten für den Datenschutz über Stichprobenkontrollen entweder vorab zu informieren oder ihn einzubinden, um die Einhaltung der datenschutzrechtlichen Festlegungen transparent machen zu können.

Die Geschäftsleitung nahm die Anregungen des TLfDI auf und passte die Arbeitsanweisung in dem Punkt an. Vor einer geplanten Kontrolle von Beschäftigten ist der Beauftragte für den Datenschutz nunmehr mit einem Vorlauf von mindestens zwei Werktagen zu informieren. Nach Abschluss der Kontrollmaßnahmen ist dem Beauftragten für den Datenschutz ein Protokoll der Durchführung und Ergebnisse auszuhändigen. Die Beschäftigten sind innerhalb von vierzehn Tagen über die durchgeführte Überprüfung und den Umfang der dabei erhobenen Daten zu informieren.

Der Einsatz von GPS ist zum Schutz bei Diebstahl des Fahrzeugs, zu Abrechnungszwecken gegenüber den Kunden und zur Optimierung des Einsatzes bzw. für die Routenplanung zulässig. Eine Dauerüberwachung von Mitarbeitern ist aufgrund des permanenten Kontrolldrucks unzulässig. Für die Fahrzeugführer muss erkennbar sein, ob und in welchem Umfang ihre personenbezogenen Daten verarbeitet oder genutzt werden. Stichproben oder Kontrollen bei konkretem Verdacht sind zulässig.

7.5 Was ist vor der Inbetriebnahme einer Kamerainstallation zu beachten?

Ein anonymes Schreiben erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Darin wird von einem Betrieb berichtet, der seine Produktionshallen von innen und außen mit Videokameras überwacht. Die Mitarbeiter beschwerten sich zwar darüber, seien aber zu einer Einverständniserklärung genötigt worden. Seitens der Geschäftsführung werde die Videoüberwachung als versicherungstechnisch erforderlich gerechtfertigt. Zudem wurden dort elektronische Schlüssel eingeführt, welche auch für den Zugang zu den Umkleieräumen und den Toiletten zu benutzen sind. Mittels dieser Schlüssel könne laut Geschäftsleitung ausgelesen und gespeichert werden, welcher Mitarbeiter welche

Tür wie oft benutzt. Der Beschwerdeführer wandte sich deshalb mit der Bitte, die Rechtmäßigkeit der Überwachungsmaßnahme der Geschäftsleitung zu prüfen, an den TLfDI.

Aufgrund dieser Informationen beschloss der TLfDI, eine Kontrolle nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) bei dem Betrieb durchzuführen. Dabei stellte der TLfDI fest, dass an dem Standort über 20 Kameras betrieben wurden.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

In Bereichen, die nicht-öffentlich zugänglich sind, sich aber Mitarbeiter aufhalten, ist die Videoüberwachung nach § 28 BDSG zu beurteilen. Dabei muss der Einsatz von Videotechnik zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. So können ausnahmsweise Eigentümerinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn Beschäftigte nicht im Fokus der Überwachung stehen und nicht permanent überwacht werden. In diesem Fall befanden sich aber einige Kameras an den Arbeitsplätzen der Beschäftigten, sodass sich diese hauptsächlich im Aufnahmebereich befanden und damit die Voraussetzungen für die Verarbeitung von Beschäftigtendaten nach § 32 BDSG hätten vorliegen müssen, was nicht der Fall war. Um die Eigentümerinteressen zu begründen, führte der Geschäftsführer an, dass es in den letzten zwei Jahren fünf Einbrüche in die Firma gegeben hätte.

Außerdem haben nach § 4f Abs. 1 BDSG nicht-öffentliche Stellen, die eine automatisierte Verarbeitung vornehmen, einen betrieblichen Datenschutzbeauftragten zu bestellen, es sei denn, es sind in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, § 4f Abs. 1 Satz 4 BDSG. Diese Ausnahme griff aber im vorliegenden Fall nicht, weil mit dem Betrieb der Videoüberwachung besondere Risiken für die Rechte und Freiheiten der Betroffenen verbunden sind, § 4f Abs. 1 Satz 6 BDSG i. V. m. § 4d Abs. 5 BDSG.

Einen betrieblichen Datenschutzbeauftragten gab es in dem Betrieb nicht. Zum Beauftragten für den Datenschutz darf nach § 4d Abs. 2 Satz 1 BDSG nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Neben der fachlichen Qualifikation ist daher wichtig, dass der betriebliche

Datenschutzbeauftragte aufgrund seiner persönlichen Eigenschaften sowie seines Verhaltens geeignet ist, seine Aufgaben ordnungsgemäß zu erfüllen. Die Firma bestellte die Leiterin der Datenverarbeitung als betriebliche Datenschutzbeauftragte. Diese kommt jedoch aufgrund ihres beruflichen Aufgabengebiets in einen Interessenkonflikt. Der TLfDI forderte daher, eine andere Person zum betrieblichen Datenschutzbeauftragten zu bestellen.

Außerdem ist gemäß § 4d Abs. 5 BDSG eine Vorabkontrolle erforderlich, wenn die automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Hiervon ist nach den bei der Kontrolle gemachten Feststellungen auszugehen. Diese Vorabkontrolle wäre durch den betrieblichen Datenschutzbeauftragten durchzuführen gewesen. Hier war zur Zeit der Inbetriebnahme kein Datenschutzbeauftragter bestellt, deshalb hätte dem TLfDI eine Meldung nach § 4d Abs. 1 BDSG gemacht werden müssen, auch dies ist nicht erfolgt.

Des Weiteren ist durch den betrieblichen Datenschutzbeauftragten eine Verfahrensübersicht, gemäß § 4g Abs. 2 und 2a BDSG, zu erstellen, die darin aufzunehmenden Angaben zählt der § 4e Satz 1 BDSG auf. Eine solche Verfahrensübersicht ist auch für das Schließsystem an zu fertigen. Um eine solche Verfahrensübersicht zu erstellen, wurden dem Betrieb vom TLfDI entsprechende Formulare zum Ausfüllen übersandt.

In diesen Formularen gab der Betrieb an, dass eine Löschung der Daten alle sieben Tage geschehe. Jedoch sind gemäß § 6b Abs. 5 BDSG die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Der TLfDI hielt im vorliegenden Fall eine Speicherdauer von 72 Stunden für angemessen, weil sich während des Wochenendes keine Personen im Betrieb aufhielten. Während der Betriebsferien könne die Speicherdauer erhöht werden.

Der TLfDI steht noch mit dem Betrieb in Kontakt, es wurden noch weitere und konkretere Auskünfte vom Betrieb verlangt, um die Zulässigkeit der Maßnahme der Videoüberwachung datenschutz-

rechtlich beurteilen zu können. Die Prüfung der Unterlagen war zum Ende des Berichtszeitraums noch nicht abgeschlossen.
Ein Bußgeldverfahren wird sich anschließen.

Nach § 4f Abs. 1 BDSG haben Betriebe einen Beauftragten für den Datenschutz zu bestellen. Durch diesen ist gemäß § 4d Abs. 5 BDSG eine Prüfung der automatischen Verarbeitung vor Beginn der Verarbeitung durchzuführen, wenn die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist. Sollte kein betrieblicher Datenschutzbeauftragter bestellt worden sein, ist der Aufsichtsbehörde nach § 4d Abs. 1 BDSG eine Meldung zu machen.

7.6 Datenschutz in der Altenhilfe: Wer hat wo- wann- wem geholfen?

Im Januar 2015 wandte sich eine Einrichtung der Altenhilfe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Informationen zum Umgang mit Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen insbesondere im Hinblick auf haftungsrechtliche Konsequenzen. In der Anfrage wurde dargelegt, dass sich in den einschlägigen Gesetzen für diese Dokumente keine speziellen Regelungen fänden.

Der TLfDI beantwortete die Anfrage folgendermaßen:

Tatsächlich gibt es hinsichtlich der Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen in den Einrichtungen der Altenhilfe keine speziellen gesetzlichen Regelungen. Da diese Dokumente jedoch allesamt personenbezogene Daten enthalten, ist hierfür das Bundesdatenschutzgesetz (BDSG) anwendbar. Nach § 20 Abs. 2 BDSG müssen personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, gelöscht werden, wenn ihre Speicherung unzulässig ist oder wenn die verantwortliche Stelle diese Daten für die Erledigung ihrer Aufgaben nicht mehr benötigt. Gemäß § 20 Abs. 3 BDSG ist in folgenden Fällen anstelle der Löschung eine Sperrung der Daten vorgesehen:

- wenn einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
- wenn Grund zur Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden,

- wenn eine Löschung wegen der besonderen Speicherart nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Bei den angegebenen Dokumenten handelt es sich um nicht automatisierte Dateien. Grundsätzlich sind diese Dokumente zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Stundenabrechnungen können solange aufbewahrt werden, bis die entsprechenden Beträge bezahlt sind. Auch danach ist eine Aufbewahrung möglich, um eventuell bestehende Meinungsverschiedenheiten zu klären, sofern Verjährungs- bzw. Rechtsmittelfristen noch nicht abgelaufen sind. Dies gilt ebenso für Dienst- und Tourenpläne. Dabei ist jedoch zu beachten, ob allgemeine gesetzliche Aufbewahrungsfristen nach dem Handels- oder Steuerrecht zu beachten sind und die Akten dann nach § 20 Abs. 3 BDSG gesperrt werden müssen. Nach § 3 Abs. 4 Nr. 4 BDSG bedeutet „Sperrung“, dass die gespeicherten personenbezogenen Daten entsprechend gekennzeichnet werden müssen, um ihre Weiterverarbeitung oder -nutzung einzuschränken. Es sind nach § 9 BDSG organisatorische Maßnahmen zu treffen, dass diese Akten dem Zugriff der Mitarbeiter im Rahmen der normalen Bearbeitung entzogen werden. Dies kann beispielsweise durch die Einlagerung in einen Archivraum geschehen, zu dem nur ein begrenzter Mitarbeiterkreis Zugang hat.

Hinsichtlich der Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen in der Altenhilfe gilt das Bundesdatenschutzgesetz (BDSG). Nach § 20 Abs. 2 BDSG müssen diese Daten gelöscht werden, wenn die verantwortliche Stelle die Daten zur ordnungsgemäßen Erledigung ihrer Aufgaben nicht mehr benötigt. In Einzelfällen können einer Löschung der Daten gesetzlich geregelte Aufbewahrungsfristen entgegenstehen (beispielsweise nach dem HGB). In diesen Fällen sind die Daten gemäß § 20 Abs. 3 BDSG zu sperren und in ein gesichertes Archiv zu überführen.

7.7 Bewerbungsverfahren abgeschlossen – Bewerberdaten gelöscht?

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Unternehmen der Bitte, seine personenbezogenen Daten zu löschen, nicht nachgekommen sei. Der Beschwerdeführer hatte sich bei dem Unternehmen beworben und ein Absageschreiben erhalten.

Daraufhin bat er das Unternehmen wiederholt per E-Mail darum, seine personenbezogenen Daten, auch die intern an den Geschäftsführer weitergeleiteten Daten und entsprechende Ausdrucke, zu löschen bzw. zu vernichten und ihm die Löschung zu bestätigen. Eine derartige Bestätigung hatte er aber nicht erhalten.

Der TLfDI ist gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) dazu ermächtigt, die Ausführung des BDSG und anderer Vorschriften über den Datenschutz zu kontrollieren (§ 38 Abs. 1 Satz 1 BDSG). Der Zweck dieser Kontrolle ist es, den Betroffenen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 24 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Personenbezogene Daten sind zu löschen, wenn die Voraussetzungen des § 35 Abs. 2 BDSG vorliegen. Unter anderem ist danach eine Löschung erforderlich, wenn die Kenntnis der Daten für die Erfüllung der Zwecke, für die sie erhoben wurden, nicht mehr erforderlich ist (Nummer 3).

In Ausübung seiner Kontrollfunktion bat der TLfDI das Unternehmen um eine detaillierte Auskunft zum vorgetragenen Sachverhalt des Beschwerdeführers gemäß § 38 Abs. 3 BDSG. Ergänzend wies der TLfDI in diesem Zusammenhang darauf hin, dass es sich auch bei den Anfragen des Beschwerdeführers um personenbezogene Daten handelt, die gegebenenfalls nach Bearbeitung seiner Beschwerde zu löschen sind. Sollten im Unternehmen schriftliche Festlegungen zum Umgang mit Bewerberdaten nach Abschluss des Verfahrens vorliegen, bat der TLfDI um Übersendung einer Kopie.

Auf seine Anfrage teilte das Unternehmen dem TLfDI mit, dass alle personenbezogenen Daten und Anfragen des Beschwerdeführers nach Abschluss des Bewerbungsverfahrens gelöscht worden seien. Das Unternehmen habe den Beschwerdeführer nicht über die Löschung informiert, da es von dessen Seite nach eigener Darlegung keine entsprechende Aufforderung erhalten habe. Der TLfDI informierte den Beschwerdeführer über die durch das Unternehmen bestätigte Löschung seiner gesamten personenbezogenen Daten und Anfragen und legte dar, dass insofern keine Anhaltspunkte für datenschutzrechtliche Verstöße bestehen. Da der Beschwerdeführer sich nicht mehr meldete, konnte der Vorgang abgeschlossen werden.

Nach § 24 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Personenbezogene Daten sind nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, wenn die Kenntnis der Daten für die Erfüllung der Zwecke, für die sie erhoben wurden nicht mehr erforderlich ist. Dies ist in der Regel bei einer erfolglosen Bewerbung der Fall.

7.8 Wenn der Chef weiß, dass der Mitarbeiter zur Konkurrenz will

Im September 2015 wandte sich eine Arbeitnehmerin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Auskunft, inwiefern ein fremdes Unternehmen, bei dem sie sich beworben hatte, dazu befugt ist, über diese Bewerbung das Unternehmen, bei dem sie angestellt ist, in Kenntnis zu setzen. Die Geschäftsführung des Unternehmens, bei dem die Beschwerdeführerin angestellt war, hatte ihr in einem persönlichen Gespräch vorgeworfen, auf der Suche nach einem neuen Tätigkeitsfeld als Immobilienverwalterin zu sein. Hierüber hatte sich der Geschäftsführer geärgert und der Arbeitnehmerin einen Aufhebungsvertrag angeboten. Auf Nachfrage bei dem Geschäftsführer, woher er die Informationen erhalten habe, erhielt die Beschwerdeführerin keine Auskunft. Bei diesem Gespräch waren zwei weitere Personen anwesend.

Die Beschwerdeführerin hatte sich bei einem Personaldienstleister auf eine ausgeschriebene Stelle beworben. Was sie nicht wusste: Diese Stelle war für die Firma, in der die Beschwerdeführerin aktuell beschäftigt war, ausgeschrieben. Die Beschwerdeführerin vermutete, dass der Personaldienstleister die entsprechenden Informationen weitergegeben hatte, zumal ihre Firma wohl ausschließlich mit diesem Personaldienstleister zusammenarbeitete. Die Beschwerdeführerin hatte nach eigener Aussage bereits einen Anwalt kontaktiert und dargelegt, dass der Personaldienstleister ihre Daten nicht an den Geschäftsführer hätte weitergeben dürfen.

Die Arbeitnehmerin erbat vom TLfDI Auskunft darüber, ob gegen ihren Arbeitgeber und den Personaldienstleister aus datenschutzrechtlichen Gründen etwas unternommen werden könne. Der TLfDI kam nach der datenschutzrechtlichen Prüfung zu dem Ergebnis, dass eine Datenverarbeitung im Auftrag nicht vorlag, weil die Arbeit-

nehmerin unmittelbar einen Vertrag mit dem Arbeitsvermittler geschlossen hatte. Gegenstand dieses Vertrages waren nicht Daten Dritter, sondern nur ihre personenbezogenen Daten. Auch zwischen dem Unternehmen und dem Arbeitsvermittler lag kein Auftragsdatenverhältnis vor, da die Stellenausschreibung ohne personenbezogene Daten erfolgte. Der TLfDI antwortete der Arbeitnehmerin folgendermaßen:

Der Vorgesetzte der Beschwerdeführerin hätte von vornherein die Informationen über anderweitige Bewerbungen gar nicht erheben dürfen. Nach § 32 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten über Beschäftigte für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder für dessen Beendigung erforderlich ist. Eine Notwendigkeit für die Durchführung oder Beendigung des Beschäftigungsverhältnisses lag nicht vor, da die Bewerbung bei einem anderen Unternehmen arbeitsrechtlich kein anerkannter Kündigungsgrund ist. Die Arbeitnehmerin hatte sich auf die vom Personaldienstleister ausgeschriebene Stelle beworben, da sie nicht wissen konnte, dass der Personaldienstleister die Stelle im Auftrag ihres derzeitigen Arbeitgebers ausgeschrieben hatte. Für den Personaldienstleister hingegen wäre es nicht erforderlich gewesen, die Geschäftsführer über den Veränderungswunsch ihrer Mitarbeiterin zu informieren, da die Begründung eines weiteren Arbeitsverhältnisses bei dem gleichen Unternehmen sicher nicht zur Debatte stand.

Nach § 34 BDSG hat ein Betroffener das Recht, von der verantwortlichen Stelle Auskunft über die zu seiner Person gespeicherten Daten zu verlangen, das heißt, die Beschwerdeführerin kann von ihrem Beschäftigungsunternehmen eine direkte Auskunft dazu fordern, woher der Geschäftsführer seine Informationen hatte. Allerdings ist es auch hier sehr wahrscheinlich, dass die Angabe über die anderweitige Bewerbung nirgendwo schriftlich dargelegt und eine Überprüfbarkeit somit nicht möglich ist.

Ein datenschutzrechtlich überprüfbarer Aspekt ist jedoch die Tatsache, dass das gesamte Gespräch zwischen der Arbeitnehmerin und der Geschäftsführung (Arbeitgeber) unter zwei Zeugen stattfand, insbesondere, wenn dabei der berufliche Veränderungswunsch der Beschwerdeführerin dargelegt wurde. Dieser Veränderungswunsch hätte den anwesenden Personen (Assistenz der Geschäftsführung und Personalmitarbeiter) nicht mitgeteilt werden dürfen.

Im Hinblick darauf bot der TLfDI der Beschwerdeführerin an, diesen Aspekt nach § 38 Bundesdatenschutzgesetz gegenüber dem Beschäftigungsunternehmen aufzugreifen. Da sich die Beschwerdeführerin nicht mehr meldete und dem TLfDI das Unternehmen nicht bekannt war, konnte er in der Angelegenheit nicht weiter tätig werden.

Gemäß § 32 Abs. 1 BDSG dürfen Unternehmen personenbezogene Daten über Beschäftigte nur für Zwecke des Beschäftigungsverhältnisses erheben, verarbeiten oder nutzen, wenn dies für die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist. Daraus ergibt sich, dass ein Vorgesetzter oder Personalverantwortlicher keine Informationen darüber erheben darf ob oder inwiefern seine Mitarbeiter sich anderweitig bewerben, wenn die Mitarbeiter ihn hierüber nicht freiwillig in Kenntnis setzen. Eine anderweitige Bewerbung stellt keinen zulässigen Kündigungsgrund dar.

7.9 Betriebsärztliche Untersuchungen: keine automatische Schweigepflichtentbindung im Arbeitsvertrag

Nach § 8 Abs. 1 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (Arbeitssicherheitsgesetz – ASiG) haben auch Betriebsärzte die Regeln der ärztlichen Schweigepflicht zu beachten. Lediglich auf Wunsch des Arbeitnehmers ist nach § 3 Abs. 2 ASiG das Ergebnis arbeitsmedizinischer Untersuchungen mitzuteilen.

Die Arbeitnehmervertretung eines Thüringer Unternehmens wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da das Unternehmen dazu übergegangen war, von seinen Arbeitnehmern im Arbeitsvertrag gleichzeitig die Unterschrift zur Entbindung der Betriebsärzte von ihrer Schweigepflicht gegenüber dem Arbeitgeber zu fordern.

Nach Prüfung der entsprechenden Klausel im Arbeitsvertrag teilte der TLfDI der Arbeitnehmervertretung mit, dass der Arbeitnehmer mit der Unterschrift unter den Arbeitsvertrag mit einer Klausel zur Schweigepflichtentbindung noch keine wirksame Schweigepflichtentbindung erklärt hätte. Die Einwilligung entsprach nämlich nicht der Form nach § 4a Abs. 1 Satz 1 BDSG, denn sie war nicht besonders hervorgehoben. Weiterhin kommt eine Entbindung von der Schweigepflicht des behandelnden Arztes nur dann in Frage,

soweit der Arbeitgeber ein berechtigtes Interesse an der entsprechenden Information darlegt. Praktisch müsste der/die Betroffene also vor einer Mitteilung des behandelnden Arztes an den Arbeitgeber im Einzelfall jeweils eine Schweigepflichtentbindung erteilen bzw. kann diese auch verweigern oder einschränken. Daher war aus Sicht des TLfDI die Befürchtung der Arbeitnehmervertretung unbegründet, dass auf der Grundlage des unterschriebenen Arbeitsvertrags vom Betriebsarzt dem Arbeitgeber der ärztlichen Schweigepflicht unterliegende Einzelheiten mitgeteilt werden könnten.

Eine pauschale Schweigepflichtentbindungserklärung in einem Arbeitsvertrag ist mit der Unterschrift des Vertrags keine wirksame Einwilligung zur Datenübermittlung zwischen Betriebsarzt und Arbeitgeber. Der Betriebsarzt muss vor jeder Datenübermittlung an den Arbeitgeber eine gesonderte zweckgebundene Schweigepflichtentbindung einholen.

7.10 Auskunftspflicht von Unternehmen

Grundsätzlich hat die verantwortliche Stelle nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, deren Herkunft, den Empfänger, an den die Daten weitergegeben werden und den Zweck der Speicherung. Mit der Beantwortung von Auskunftsverlangen Betroffener machen es sich manche Unternehmen mitunter allerdings etwas zu leicht.

Ein Betroffener machte von seinem Auskunftsrecht gegenüber einem Thüringer Unternehmen Gebrauch und verlangte gleichzeitig – selbstverständlich nach Erteilung der Auskunft – die Löschung, ersatzweise Sperrung, seiner Daten. Daraufhin erhielt er die nicht näher differenzierte Auskunft, man habe die von ihm im Zusammenhang mit seiner Online-Bewerbung angegebenen Daten im internen System gespeichert, eine Weitergabe sei zum Zweck der Arbeitnehmerüberlassung erfolgt, seine Daten würden aus dem System gelöscht. Damit war der Betroffene nicht zufrieden und machte wegen unzureichender Auskunft eine Eingabe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er nämlich genau wusste, dass seine personenbezogenen Daten an ein Jobcenter in einem anderen Bundesland gelangt waren und diese Information in der Auskunft fehlte.

Der TLfDI wandte sich als Datenschutzaufsicht mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an das Unternehmen und bat unter Berufung auf die einschlägigen Auskunftsregelungen um Stellungnahme. Das Unternehmen teilte daraufhin mit, es habe dem Betroffenen nun mit ergänzender Auskunft auch mitgeteilt, zu welchem Kunden zum Zweck der Arbeitnehmerüberlassung seine Bewerbungsunterlagen weitergegeben wurden. Ob das Unternehmen auch Daten an das Jobcenter in einem anderen Bundesland übermittelt hatte, blieb zunächst noch im Dunkeln. Eine Befragung des Jobcenters zur Aufklärung war für den TLfDI mangels Zuständigkeit nicht möglich. Dies wurde dem Beschwerdeführer mitgeteilt, der sich im Übrigen seinen Angaben zufolge auch bereits an die für das besagte Jobcenter zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gewandt hatte.

Der Beschwerdeführer gab sich indes mit dem Ergebnis der Bemühungen des TLfDI nicht zufrieden, denn seiner Meinung nach war die ihm vom Unternehmen erteilte Auskunft falsch. Nach seinen Informationen, die er nun nachschob, habe es einen regelrechten Datenaustausch des Thüringer Unternehmens mit dem Jobcenter im anderen Bundesland gegeben.

Angefragt teilte daraufhin die Niederlassung des Thüringer Unternehmens in einem anderen Bundesland dem TLfDI zur Aufklärung mit, der Beschwerdeführer selbst habe gebeten, mit dem Sachbearbeiter des Jobcenters in Kontakt zu treten, um zu klären, weshalb ein Fahrkostenantrag abgelehnt worden sei. Hierfür habe er telefonisch die Kontaktdaten durchgegeben. Aufgrund der dargelegten eindeutigen Bitte war das Unternehmen auch nach Auffassung des TLfDI zu Recht davon ausgegangen, dass der Beschwerdeführer damit auch zum Anruf des Sachbearbeiters seine Einwilligung erteilt hatte.

Ob möglicherweise in dem Gespräch mit dem Sachbearbeiter beim Jobcenter weitere personenbezogene Daten zu dem Beschwerdeführer ausgetauscht wurden, wie der Beschwerdeführer vermutete, konnte aber vom TLfDI nicht weiter überprüft werden, da weder die Niederlassung des Unternehmens noch das Jobcenter seiner Datenschutzaufsicht unterlagen.

Die Auskunft an den Betroffenen nach § 34 BDSG über die zu seiner Person gespeicherten Daten umfasst auch Angaben zur Herkunft dieser Daten und die Empfänger, an die die Daten weitergegeben werden sowie den Zweck der Speicherung.

7.11 GPS für Arbeitgeber attraktiv – aber oft unzulässig

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage auf Auskunft zur Rechtmäßigkeit von Global-Positioning-System (GPS)-Ortung an Firmenfahrzeugen. Die Mitarbeiterin eines Sanitätshauses, die dort als Außenmitarbeiterin angestellt ist und ein Dienstfahrzeug nutzt, wünschte Auskunft zur datenschutzrechtlichen Zulässigkeit der GPS-Überwachung des Fahrzeuges.

Da sie den Sachverhalt nicht genauer schilderte, konnte der TLfDI nur eine allgemeine Auskunft erteilen. Durch den Einsatz von GPS-Technik werden Standortdaten erfasst, aufgrund derer Bewegungsprofile erstellt werden können. Es gilt daher, eine unzulässige Mitarbeiterüberwachung zu verhindern.

Grundsätzlich ist der Einsatz von GPS an Firmenfahrzeugen zulässig, sofern dies für eine Feststellung von Einsätzen, beispielsweise zu Abrechnungszwecken, erforderlich ist. In jedem Fall ist eine schriftliche Festlegung notwendig, die beinhaltet, in welchem Umfang und unter welchen Voraussetzungen Positionsdaten eines Fahrzeuges von einem bestimmten Personenkreis festgestellt und genutzt werden dürfen. Solche Festlegungen müssen aus Gründen der Transparenz dem Fahrzeugnutzer offengelegt und in einer Dienstvereinbarung abgestimmt werden.

Es kann zum Beispiel zulässig sein, GPS-Daten für steuerliche Zwecke auszudrucken. Diese Angaben ersetzen dann das früher übliche Fahrtenbuch. Dagegen wäre es unzulässig, wenn anhand der GPS-Positionsdaten ein lückenloses Bewegungsprofil ständig (auch für die Vergangenheit) einsehbar ist und damit eine vollständige Leistungs- und Verhaltenskontrolle vom Arbeitgeber ausgeübt wird.

Unzulässig sind auch Auswertungsfunktionalitäten, die nur einer persönlichen Überwachung von Beschäftigten dienen können, etwa Geschwindigkeitsaufzeichnungen und im Außendienst auch die Dauer von Fahrtunterbrechungen. Derartige Funktionen sind in der Regel technisch zu unterbinden, um die Mitarbeiter nicht einem permanenten Kontrolldruck auszusetzen.

Bei der Nutzung von GPS-Technik in einem Firmenwagen muss vom Arbeitgeber offengelegt werden, welche Daten für welchen Zweck erhoben werden, wie lange sie gespeichert werden dürfen und

zu welchem Zweck sie genutzt werden sollen. Ein lückenloses Bewegungsprofil ist wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig.

7.12 Lehrlinge im Fokus – kein Videogaga bei Nichterkennbarkeit

Ein Thüringer Unternehmen richtete eine neue Lehrwerkstatt ein. Weil man Arbeitsunfälle befürchtete und der Lehrausbilder nicht ständig präsent sein konnte, wollte man auf die technischen Möglichkeiten zurückgreifen und eine Videoüberwachung installieren. Eine Verhaltenskontrolle der Lehrlinge wollte man natürlich nicht. Zugriff auf das Videomaterial sollte auch nur der Lehrausbilder und daneben auch der Empfang haben, denn Letzterer war ständig besetzt, um gegebenenfalls Hilfe zu organisieren. Der Betriebsrat des Unternehmens bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Einschätzung der Zulässigkeit des Vorhabens und um Beratung.



Der TLfDI verwies zunächst auf die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ in der die Datenschutzaufsichtsbehörden der Länder die Grundsätze für eine datenschutzkonforme Videoüberwachung festgelegt haben. Diese Orientierungshilfe ist auf der Homepage des TLfDI unter <https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v-durch-nicht-ffentliche-stellen.pdf> für jedermann abrufbar.

Die Videoüberwachung von Arbeitnehmern ist, wie in der Orientierungshilfe dargestellt, nur unter sehr engen Voraussetzungen möglich. Bei sicherheitsrelevanten Belangen müssen diese konkret dargestellt werden. Allein die Befürchtung, es könnte aufgrund von Unerfahrenheit zu Arbeitsunfällen kommen, reicht nicht aus. Auch ist eine Videoüberwachung nicht geeignet, Arbeitsunfälle zu verhindern. Darüber hinaus war auf den Fall bezogen nicht klar, weshalb Lehrausbilder und Empfang Zugriff auf die Bilder haben sollten. Alle Aspekte sind im Rahmen einer Vorabkontrolle nach § 4d Abs. 5 Bundesdatenschutzgesetz (BDSG) durch den für das Unternehmen bestellten Datenschutzbeauftragten zu prüfen.

Der Betriebsrat teilte dann mit, aufgrund der Hinweise und Beratung durch den TLfDI habe man sich dazu entschieden, ein reines Monitoring einzurichten, weil die hohe Verletzungsgefahr durch die Nutzung der Holzverarbeitungsmaschinen im Lehrbereich bestehe und man eine Nothilfe sicherstellen wolle. Die dort anwesenden Personen seien durch einen Schleier, den man über zu übertragende Bilder gelegt habe, nicht mehr erkennbar. Damit sei sichergestellt, dass sobald der Stillstand von Maschinen oder Personen erkennbar werde, Hilfe geleistet werden könne. Damit war das Vorhaben aus datenschutzrechtlicher Sicht als akzeptabel anzusehen.

Ein reines Monitoring eines Unternehmensbereiches, in dem hohe Verletzungsgefahr besteht, ist unter der Voraussetzung, dass Personen grundsätzlich nicht erkennbar sind und damit eine Leistungs- und Verhaltenskontrolle ausgeschlossen werden kann, aus datenschutzrechtlicher Sicht zulässig.

7.13 Anfrage zum Passwortschutz von Arbeitsplatzrechnern

Ein interessierter Bürger bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Informationen dazu, wie Passwörter an Arbeitsplatzrechnern möglichst datenschutzgerecht gestaltet werden können. Konkret wollte er wissen, inwiefern ein Arbeitgeber seinen Beschäftigten die Möglichkeit einräumen muss, das Passwort am Arbeitscomputer ändern zu können.

Hierzu teilte der TLfDI mit, dass der Arbeitgeber jedem seiner Beschäftigten die Möglichkeit einräumen muss, eine Passwortänderung an seinem Arbeitsrechner durchführen zu können. Nach § 9 Bundesdatenschutzgesetz (BDSG) hat die Stelle, die die personenbezogenen Daten erhebt, verarbeitet und nutzt (verantwortliche Stelle), die technischen und organisatorischen Maßnahmen zu treffen, die nötig sind, um die datenschutzrechtlichen Vorgaben einzuhalten. Es muss nach Nummer 2 der Anlage zu § 9 BDSG insbesondere verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle). Mitarbeiterpasswörter dürfen nur dem Mitarbeiter selbst bekannt sein und dürfen daher auch grundsätzlich nicht bei Dritten hinterlegt werden. Entscheidend ist, dass solche Passwörter dabei nicht an Dritte, also auch nicht an den Vorgesetzten, weitergegeben werden. Das Bundesamt für die Sicherheit

in der Informationstechnik (BSI) empfiehlt unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz/Kataloge/Inhalt/_content/m/m02/m02011.html unter anderem folgende Maßnahmen zu Passwortgestaltung und -gebrauch:

Das Passwort darf nicht leicht zu erraten sein.

- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Zeichenarten verwendet werden.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.
- Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner wirklich überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Passwörter müssen geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss.
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.



Laut § 9 BDSG muss die Daten erhebende Stelle alle technischen und organisatorischen Maßnahmen treffen, um die datenschutzrechtlichen Vorgaben einzuhalten. Hierzu zählen auch die Zugangskontrolle und die Zugriffskontrolle sowie die Eingabekontrolle. Daher hat jeder Mitarbeiter das Recht, sein Passwort am Arbeitsplatzrechner zu ändern. Es sind die Vorgaben des BSI für die Vergabe von Passwörtern zu beachten.

7.14 Veröffentlichen von Bildern behinderter Menschen

Eine Behinderteneinrichtung fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob es datenschutzrechtlich zulässig ist, wenn sie Bilder von der Tätigkeit der Behinderten in den Werkstätten auf den Fluren der Einrichtung aushängt und somit veröffentlicht. Auch wollten sie zur Freude der Behinderten die Bilder von Weihnachtsfeiern aushängen. Jedoch zweifelte die Behinderteneinrichtung, dass es überhaupt möglich ist, die Einwilligungserklärung von einigen einzuholen, da Zweifel hinsichtlich der Geschäftsfähigkeit bestünden.

Der TLfDI nahm hierzu wie folgt Stellung:

Das Recht am eigenen Bild ist ein Spezialfall des Rechts auf informationelle Selbstbestimmung und wird durch das Kunsturheberrechtsgesetz (KunstUrhG) geschützt. Gemäß § 22 Kunsturhebergesetz dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von zehn Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Ein Arbeitgeber darf Bilder seiner Beschäftigten, nach § 3 Abs. 11 Nr. 4 Bundesdatenschutzgesetz (BDSG) sind auch behinderte Menschen in anerkannten Werkstätten Beschäftigte, entsprechend der oben zitierten Bestimmung nur mit der Einwilligung verbreiten, etwa in Broschüren oder auf der Intra- oder Internetseite des Unternehmens (vgl. Auernhammer / Forst BDSG-Kommentar 4. Auflage, § 32 Rdnr. 68). Es muss also eine Einwilligung der Betroffenen vorliegen. Nach § 4a BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Einwilligung ist eine rechtsgeschäftliche Erklärung bei der es darauf ankommt, ob die Betroffenen in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu überblicken und sich daher verbindlich dazu äußern zu können (Simitis in: Simitis, BDSG Kommentar, 8. Auflage, § 4a Rdnr. 20). Der TLfDI entnahm der Darstellung der Einrichtung, dass einige Beschäftigte nicht über die erforderliche Einsichtsfähigkeit verfügen, um die Tragweite ihrer Einwilligung zu überblicken. In diesem Fall fällt dem auch für arbeitsrechtliche

Sachverhalte bestellten Betreuer als gesetzlicher Vertretung die Aufgabe zu, über die Erteilung einer Einwilligung zu entscheiden.

Im Ergebnis muss vor einer Veröffentlichung von Aufnahmen, auf denen Arbeitnehmer einer Werkstätte zu erkennen sind, eine Einwilligung eingeholt werden. Bei geschäftsunfähigen Arbeitnehmern ist der Betreuer um die Einwilligung zu ersuchen. Bei geschäftsfähigen Arbeitnehmern ist eine in § 4a BDSG geregelte Einwilligung einzuholen, soweit dies möglich ist. Kann der Betroffene z. B. nicht schreiben, kann die Willensbekundung auch vom Betreuer schriftlich festgehalten werden. Ist die Behinderteneinrichtung der Auffassung, dass der Betroffene den Sinn der Einwilligung nicht erfasst, so muss sie sich zur Klärung über den Fortgang der Angelegenheit an dessen Betreuer wenden.

7.15 Beschäftigtendatenschutz – lückenlose Leistungs- und Verhaltenskontrolle unzulässig

Die Datenschutzbeauftragte eines Thüringer Unternehmens wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), und wollte wissen, welche personenbezogenen Daten eines Mitarbeiters (zum Beispiel zur Arbeitsleistung, Ausnutzung der Arbeitszeit, Effektivität der Arbeit, Motivation) innerhalb der Firma zum Beispiel an den Vorgesetzten oder die gesamte Abteilung weitergegeben werden können.

Da die Datenschutzbeauftragte keine weiteren Angaben machte, wies der TLfDI sie allgemein auf die Regelung des § 32 Bundesdatenschutzgesetz (BDSG) hin. Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Entscheidung über die Begründung oder Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist. Darüber hinaus kann der Betriebsrat interne Festlegungen treffen. Außerdem müssen gegebenenfalls tarifrechtliche Regelungen einbezogen werden. Allerdings gilt immer, dass eine lückenlose Leistungs- und Verhaltenskontrolle nicht zulässig ist. Insgesamt kommt es regelmäßig auf den jeweiligen Einzelfall an. Da die Anfrage ein sehr weites Feld des Beschäftigtendatenschutzes betraf, konnte sie ohne Kenntnis näherer Umstände nicht in der gebotenen Ausführlichkeit beantwortet werden. Der Datenschutzbeauftragten wurde angeboten, konkrete Einzelfragen an

den TLfDI zu richten oder nähere Angaben zum Sachverhalt zu machen. Offenbar genügte die gegebene Auskunft, sodass die Datenschutzbeauftragte sich nicht wieder meldete.

Im Bereich des Beschäftigungsverhältnisses findet der § 32 BDSG Anwendung, grundsätzlich dürfen danach personenbezogene Daten für den Zweck des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

7.16 Satte Rabatte contra Beschäftigtendatenschutz

Ein großer Discounter mit Filialen in Thüringen hatte im Herbst 2015 mit einer Rabattaktion geworben. Dabei konnte der Kunde selbst bestimmen, auf welche Artikel er welchen Rabatt geltend machen wollte. Hierfür wurden Werbebögen mit Aufklebern verteilt, damit die Kunden auf von ihnen ausgewählter Ware Rabatte bis zu 20 Prozent erhalten konnten. Pro Einkauf durften jedoch maximal zehn Coupons, so viele wie auf dem Werbebogen enthalten, eingelöst werden.

Da die Kassen offenbar die Anzahl der eingelösten Rabatte nicht automatisch erkennen konnten, wurden die Mitarbeiter belehrt, dass mit arbeitsrechtlichen Konsequenzen zu rechnen sei, falls die Einlösung der Rabatte nicht genau nach den Vorgaben für die Kunden erfolgte, nämlich pro Einkauf maximal nur einmal 20 Prozent, drei mal 10 Prozent und sechs mal 5 Prozent Rabatt.

Um der Androhung Taten folgen zu lassen, erfolgte eine mitarbeiterbezogene Auswertung der Kassenbons. Hatte ein Kunde mehr als die auf einem Werbebogen enthaltenen Rabatte bei einem Einkauf genutzt, wurde das Kassenspersonal unter Androhung empfindlicher Konsequenzen zur Stellungnahme aufgefordert. Über dieses Vorgehen erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einen Hinweis. Nach Auffassung des Hinweisgebers musste eine Kassenauswertung in Form einer Leistungs- und Verhaltenskontrolle ausgeschlossen sein, denn nach seinen Informationen war dies in einer entsprechenden Betriebsanweisung so festgelegt. Der TLfDI wandte sich daher als Datenschutzaufsicht nach § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz

(BDSG) an die regionale Thüringer Vertriebsleitung und verlangte Auskunft.

Vom Hauptsitz des Unternehmens erklärte man, in der Revision der Zentrale habe man zunächst eine anonyme Statistik für alle Filialen gefertigt. Als man zu dem Ergebnis kam, dass auf einem Bon unerlaubter Weise mehrere 20 Prozent Gutscheine aus der Aktion eingelöst worden waren, sollten die Regionalrevisoren prüfen, welcher Kassenbediener den Bon erstellt hatte. Dabei habe man in erster Linie Fehlbedienungen frühzeitig erkennen und Nachschulungen der Mitarbeiter veranlassen wollen, was nach § 32 Abs. 1 Satz 1 BDSG, nämlich zur Durchführung des Beschäftigungsverhältnisses, möglich sei. Da diese Auswertung aber auch einen konkreten Verdacht auf Straftaten der Kassenmitarbeiter begründet hätte, sei § 32 Abs. 1 Satz 2 BDSG einschlägig. Danach können zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an einem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Ob diese Voraussetzungen vorlagen, war letztendlich nicht durch den TLfDI zu prüfen, da die gegenständlichen personenbezogenen Auswertungen nach Versicherung der Zentrale auf deren Veranlassung erstellt wurden. Nach § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz ist nämlich der TLfDI als Datenschutzaufsicht für Betriebsstätten nur dann zuständig, wenn diese in eigener Verantwortung die personenbezogene Auswertung durchgeführt haben. Mangels eigener Befugnis der Filiale war damit die Datenschutzaufsicht am Sitz der Zentrale für die weitere Prüfung zuständig. Die Angelegenheit wurde folglich an die zuständige Datenschutzaufsicht in einem anderen Bundesland am Sitz der Zentrale abgegeben. Diese teilte nach Prüfung mit, dass sie die Vorgehensweise für vertretbar hielt, da es den Arbeitgebern möglich sein muss, im Rahmen des § 32 Abs. 1 Satz 1 BDSG nach Belehrung die Einhaltung der Vorgaben zu kontrollieren.

Datenschutzrechtliche Vorschriften verhindern bei konkreten Anhaltspunkten für nicht vorgabenkonformes Vorgehen der Beschäftigten eine konkrete personenbezogene Überprüfung nicht. Folgt eine Betriebsstätte in Thüringen den bindenden Anforderungen der Zentrale in einem anderen Bundesland und hat die Betriebsstätte keine eigenen Handlungsspielräume bei der Verarbeitung von Beschäftigtendaten, ist die Datenschutzaufsicht am Sitz der Zentrale zuständig.

7.17 Arbeitszeitüberwachung: nur datenschutzgerecht, wenn ... – Videogaga 32

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) anonym um datenschutzrechtliche Beratung gebeten. Der Sachverhalt wurde wie folgt geschildert. Ein in einer Notrufserviceleitstelle (NSL) eingesetzter Mitarbeiter überwache mitunter auch Techniker bei der Störungsbeseitigung. Das sei den Technikern bewusst, da sie in ihrem Arbeitsvertrag darüber informiert würden. Im Tätigkeitsbereich der Techniker befänden sich auch Automaten, die zum Schutz vor Vandalismus kameraüberwacht seien.

Im Störfall wenden sich die Kunden an die NSL, dann spult der NSL-Mitarbeiter vom Livebildmodus zur Zeit des Störungsauftritts zurück und gibt dem Techniker eine Information über den Vorfall. Nachdem die Störung behoben wurde, wird normalerweise der Techniker angerufen und es wird nachgefragt, wie lange er brauche, um die Störung zu beseitigen. Diese Zeit wird dann von der NSL in ein dafür vorhergesehenes Protokoll eingetragen. Wird dieser Vorgang aufgrund des Schichtsystems versäumt, kontrolliert der NSL-Mitarbeiter die Kameraaufnahmen zur Zeit der Störungsbeseitigung und trägt dann die festgestellte Zeit in das Protokoll ein.

Allerdings werde die Störung auch im Programm der Automaten angezeigt, dort seien auch die Zeit der Störung sowie die Zeit der Beseitigung der Störung ersichtlich. Ein Techniker fühle sich durch diesen Ablauf überwacht und brächte seine Beschwerde dem Betriebsrat des Unternehmens vor.

Es wurde nun darum gebeten, die datenschutzrechtliche Zulässigkeit des zum Einsatz kommenden Verfahrens der Überprüfung der Arbeitszeit festzustellen.

Da die Anfrage sehr allgemein gehalten war und keine weiteren Informationen enthielt, fasste der TLfDI die in Betracht kommenden

datenschutzrechtlichen Aspekte wie folgt zusammen: Bevor eine Kamera installiert wird und eine Videoüberwachung stattfindet, sollte das Risiko für das informelle Selbstbestimmungsrecht der Betroffenen berücksichtigt und geprüft werden, ob eine Installation überhaupt nach einer Rechtsgrundlage zulässig ist. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung nicht-öffentlich zugänglicher Räume müssen die Voraussetzungen des § 28 BDSG beziehungsweise bei gezielter Erhebung von Beschäftigtendaten die Voraussetzungen des § 32 BDSG vorliegen. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ (www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v_-durch-nicht-ffentliche-stellen.pdf). Ob eine Videoüberwachung in diesem Fall zulässig war, konnte durch den TLfDI aufgrund der geringen Informationen nicht bestimmt werden.



Der Arbeitnehmer ist durch den Arbeitsvertrag verpflichtet, in zutreffender Weise seine Arbeitszeit anzugeben. Ob dies im automatisierten Verfahren (elektronische Arbeitszeiterfassung) erfolgt oder ob hierzu handschriftliche Aufzeichnungen anzufertigen sind, kann der Unternehmer bestimmen. Die Erhebung und Verarbeitung der Arbeitsdaten ist nach § 32 Abs. 1 Satz 1 BDSG zulässig, sie sind für die Durchführung des Beschäftigtenverhältnisses erforderlich. Ein datenschutzrechtlicher Schutz dagegen, dass der Arbeitgeber im Falle von berechtigten Zweifeln an der Richtigkeit der Angabe der Arbeitszeiten eine Überprüfung vornimmt, besteht grundsätzlich nicht, denn der Arbeitgeber hat hierzu ein berechtigtes Interesse. Regelmäßig werden für solche Fälle Nachprüfungsmodalitäten festgelegt. Es kommt dabei auf die Art und Weise der Überprüfung an. Grundlage für eine rechtliche Prüfung dessen sind die entsprechenden Festlegungen des Arbeitgebers, die dem TLfDI nicht vorlagen. Der TLfDI bot an, die Angelegenheit zu prüfen und bat um nähere

Informationen. Der Anfragende bedankte sich für die Informationen und wünschte keine weitere Prüfung.

Ein Arbeitgeber kann eine Überprüfung der Arbeitszeiten vornehmen. Ob dies im automatisierten Verfahren (elektronische Arbeitszeiterfassung) erfolgt oder ob hierzu handschriftliche Aufzeichnungen anzufertigen sind, kann der Unternehmer bestimmen. Es besteht aus datenschutzrechtlichen Gründen grundsätzlich kein Schutz davor, dass, wenn der Arbeitgeber berechtigte Zweifel an der Richtigkeit der Angaben der Arbeitszeiten hegt, er eine Überprüfung derselben vornehmen kann. Regelmäßig werden für solche Fälle Nachprüfungsmodalitäten festgelegt, die einzuhalten sind.

7.18 Leistungsdruck durch GPS

Ein Mitarbeiter eines Thüringer Unternehmens wandte sich ohne konkrete Benennung seines Arbeitgebers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um Auskunft einzuholen, ob es zulässig ist, wenn der Vorgesetzte in die Firmenfahrzeuge ohne Wissen des Mitarbeiters Global-Positioning-System (GPS)-Technik einbauen lässt. Das GPS übermittelt Standortdaten, durch die Bewegungsprofile erstellt werden können. Zweck des GPS war es, nach Ansicht des Beschwerdeführers, den Mitarbeiter zu überwachen und ihn gegebenenfalls unter Druck zu setzen, falls er zu langsam arbeite.

Der TLfDI wies den Mitarbeiter auf die Regelung des § 32 Bundesdatenschutzgesetz (BDSG) hin. Danach ist die Verarbeitung von personenbezogenen Daten eines Beschäftigten nur zulässig, soweit dies zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. GPS-Nutzung ist danach nicht generell unzulässig. Durchaus können zulässige Zwecke zur Erhebung und Verarbeitung personenbezogener Daten mittels GPS vorliegen, beispielsweise die Führung eines Fahrtenbuchs für steuerliche Zwecke oder die Erhebung von Positionsdaten für besondere Einsatzzwecke in Eilfällen. Dies setzt jedoch voraus, dass die Beschäftigten entsprechend aufgeklärt sind. Da es sich um eine automatisierte Verarbeitung von personenbezogenen Daten handelt, ist in der Regel eine Vorabprüfung unter Abwägung der schutzwürdigen Interessen der Betroffenen durchzuführen. Sofern ein Betriebsrat vorhanden ist, sind die schriftlichen Festlegungen Grundlage für eine

entsprechende Betriebsvereinbarung und Betriebsanweisung. Ein lückenloses Bewegungsprofil der Mitarbeiter ist aber wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig. Von dem Angebot, sich zu melden, damit genauere Prüfungen vorgenommen werden können, machte der Beschwerdeführer keinen Gebrauch.

Sollten Mitarbeiter wahrnehmen, dass ihr Vorgesetzter heimlich Daten von ihnen durch GPS erhebt, um die Mitarbeiter auf diese Weise zu kontrollieren, können sich diese an den TLfDI wenden. Der TLfDI kann als Datenschutzaufsicht nach § 38 BDSG den Einsatz von GPS in Unternehmen mit Sitz in Thüringen konkret überprüfen. Grundsätzlich ist es zulässig, GPS-Technik in Firmenwagen zu installieren. Jedoch ist ein lückenloses Bewegungsprofil wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig.

7.19 Gab ein Arbeitsvermittler die Bewerbungsunterlagen seiner Mitarbeiterin ungefragt weiter?

Die Beschäftigte bei einem privaten Arbeitsvermittler beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie davon ausging, dass der Arbeitgeber, nachdem er das Arbeitsverhältnis in der Probezeit gekündigt hatte, sie ungefragt weitervermitteln wollte. Sie wurde nämlich von einem Unternehmen für Personaldienstleistungen angeschrieben, sie solle sich doch bitte zu ihrer Bewerbung einmal melden. Die Unterlagen seien dem Unternehmen von dem privaten Arbeitsvermittler übersandt worden. Die Betroffene war sehr erstaunt, zumal sie sich aufgrund ihres Arbeitsverhältnisses nicht anderweitig beworben hatte.

Auf die Nachfrage des TLfDI teilte der private Arbeitsvermittler mit, er habe die Personalunterlagen der bei ihm beschäftigten Beschwerdeführerin keineswegs weitergeleitet. Vor der Beschäftigung in seinem Unternehmen habe er jedoch tatsächlich die von der Beschwerdeführerin eingereichten Bewerbungsunterlagen auf eine bestimmte ausgeschriebene Stelle zur Personalvermittlung weitergereicht. Dies sei damals telefonisch in einem Interview mit der Beschwerdeführerin vor der Beschäftigung in seinem Unternehmen so vereinbart worden, denn die Betroffene habe dringend Arbeit gesucht. Das

Personaldienstleistungsunternehmen habe aber noch vor der Beschäftigung der Betroffenen dem Arbeitsvermittler per E-Mail mitgeteilt, dass die Unterlagen dort nicht weiter berücksichtigt werden könnten. Weshalb just nach der Kündigung des Arbeitsverhältnisses das Personaldienstleistungsunternehmen auf den Plan trat, war nicht zu klären.

Die Beschwerdeführerin bestritt vehement, jemals eine Einwilligung zur Weiterleitung ihrer Bewerbungsunterlagen erteilt zu haben. Sie vertrat die Auffassung, die Beweislast für das Vorliegen ihrer Einwilligung treffe ihren ehemaligen Arbeitgeber und dieser könne die erforderliche schriftliche Einwilligung nicht vorlegen, weil es keine gäbe. Sie äußerte ihr Unverständnis, dass man ihr das offenbar nicht glaube.

Eine Einwilligungserklärung ist zwar grundsätzlich schriftlich abzugeben, das Gesetz sieht aber vor, dass wegen besonderer Umstände eine andere Form angemessen sein kann (§ 4a Abs. 1 Satz 3 Bundesdatenschutzgesetz (BDSG)). Aufgrund der Schilderung des Arbeitgebers, in dem telefonischen Interview sei die Beschwerdeführerin vor ihrer Einstellung in seinem Unternehmen mit der Weitergabe der Unterlagen einverstanden gewesen, weil sie dringend Arbeit gesucht hatte, hat der TLfDI ausnahmsweise eine mündliche Einwilligung aufgrund der geschilderten Eilbedürftigkeit für angemessen angesehen. Der TLfDI wies die Beschwerdeführerin darauf hin, dass es nicht darum gehe, der einen oder anderen Seite mehr oder weniger zu glauben. Um weitergehende Schritte - also ein Bußgeldverfahren - einzuleiten, bedürfe es der Feststellung eines datenschutzrechtlichen Verstoßes. Den Darlegungen des Arbeitgebers waren jedoch keine ausreichenden Anhaltspunkte dafür zu entnehmen, dass die dem Arbeitsvermittler zugeleiteten Bewerbungsunterlagen unter Verstoß gegen datenschutzrechtliche Vorschriften der genannten Personaldienstleistungsfirma übersandt wurden.

Die Einwilligung zur Weitergabe von Bewerbungsunterlagen bedarf grundsätzlich der Schriftform, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen sein kann. Ein besonderer Umstand kann unter Umständen auch in einer eiligen Angelegenheit begründet sein. Um Missverständnisse zu vermeiden, sollte die mündlich erteilte Einwilligung nochmals schriftlich bestätigt werden.

7.20 Kündigung wegen Bewerbung in einem anderen Unternehmen?

Eine Beschäftigte in einem Handwerksbetrieb wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Vorbringen, ihr sei gekündigt worden, weil sie sich bei einem anderen Unternehmen beworben hatte. Die Chefin habe auch den anderen Kollegen ihre Bewerbung zur Kenntnis gegeben.

Damit waren Verstöße gegen datenschutzrechtliche Vorschriften sowohl seitens des Unternehmens, bei dem sich die Betroffene beworben hatte als auch seitens des Beschäftigungsunternehmens möglich. Die Bewerbungsunterlagen enthielten personenbezogene Daten der Beschäftigten, die von dem Unternehmen, bei dem sie sich beworben hatte, nur für Zwecke der Begründung eines Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden durften (§ 32 Abs. 1 Bundesdatenschutzgesetz – BDSG). Anderen Unternehmen oder einem früheren Arbeitgeber die Unterlagen weiterzuleiten ist unzulässig, da es hierfür keine gesetzliche Grundlage gibt und im vorliegenden Fall auch nicht von einer erteilten Einwilligung der Betroffenen ausgegangen werden kann, § 4 Abs. 1 BDSG. Für das beschäftigende Unternehmen besteht ebenfalls keine Befugnis, die personenbezogenen Daten einer Beschäftigten anderen Mitarbeitern zur Kenntnis geben.

Auf das Auskunftersuchen des TLfDI nach § 38 BDSG teilte das Beschäftigungsunternehmen mit, die ganzen Vorwürfe seien falsch, lückenhaft und dienten nur der Stimmungsmache. Die Bewerbungsunterlagen hätten sich eines Tages unvermittelt im Briefkasten der Geschäftsräume befunden. Es sei nicht nachvollziehbar, wer sie dort eingelegt hatte. Die Unterlagen seien inzwischen vernichtet, ohne dass sie anderen Beschäftigten zur Kenntnis gegeben worden waren. Dies war ausweislich des zugeleiteten Protokolls auch im arbeitsgerichtlichen Verfahren so vorgetragen worden.

Hat sich die Angelegenheit wie von dem Unternehmen vorgetragen abgespielt, ist kein Datenschutzverstoß durch dieses Unternehmen feststellbar. Werden einem Unternehmen ohne dessen Zutun Bewerbungsunterlagen, die an ein anderes Unternehmen gesandt wurden, zugeleitet und nutzt es diese nicht für andere Zwecke, ist kein Datenschutzverstoß erkennbar. Zeugen dafür, dass den anderen Beschäf-

tigten die Bewerbungsunterlagen zur Kenntnis gegeben wurden, hat die Beschwerdeführerin nicht benannt.

Bewerbungsunterlagen dürfen ohne Einwilligung des Bewerbers nicht an andere Stellen weitergegeben werden. Erhält ein Unternehmen ohne eigenes Zutun Kenntnis davon, dass sich ein Mitarbeiter anderweitig beworben hat, besteht keine Rechtsgrundlage dafür, diese zur Kenntnis gelangten personenbezogenen Daten des Mitarbeiters zu nutzen.

7.21 Jobsuche und alle wissen es

Eine Zeitarbeitsfirma hatte eine attraktive Stelle bei einem konkreten Unternehmen ausgeschrieben, für die sich der spätere Beschwerdeführer sehr interessierte. Also schickte er seine vollständigen Bewerbungsunterlagen, zugeschnitten auf die ausgeschriebene Stelle, an die Zeitarbeitsfirma. Kurz darauf wurde er von einem Mitarbeiter der Zeitarbeitsfirma telefonisch kontaktiert und um weitere Angaben gebeten. Dabei nahm er an, dass sich die geforderten Angaben auf die Stelle bezogen, für die er sich interessierte. Wiederum kurze Zeit später wurde er von Dritten darauf hingewiesen, dass seine personenbezogenen Daten in einem sogenannten Bewerbungsnewsletter sämtlichen Firmenkunden der Zeitarbeitsfirma zugänglich gemacht wurden. Dies umfasste neben seinem Foto, den Geburts- und Adressdaten auch die Angabe aller bisherigen Arbeitgeber inklusive der Austrittsgründe. Damit nicht genug, denn überraschenderweise besaß er nach den Angaben der Zeitarbeitsfirma besondere Fähigkeiten, von denen er bislang gar nichts gewusst hatte. Da die öffentliche Anbietung nun gar nicht seiner Intention entsprach, zog der Beschwerdeführer eiligst seine Bewerbung zurück und bat um Löschung seiner Daten, was ihm auch unverzüglich bestätigt wurde. Dennoch wurde er daraufhin weiterhin per E-Mail zum Zweck der Vermittlung angeschrieben, was eigentlich nicht möglich gewesen wäre, wenn seine Daten tatsächlich gelöscht worden wären.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, an den sich der Betroffene nun wandte, richtete ein Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz an die in Thüringen ansässige Betriebsstätte der überregionalen Zeitarbeitsfirma. Das Unternehmen teilte mit, üblicherweise erhalte ein Bewerber eine sogenannte Bewerberkarte, die einen Abschnitt „Da-

tenschutzerklärung“ enthalte, in dem darauf hingewiesen werde, dass die Daten auch anderen potenziellen Einsatzbetrieben gegeben werden können. Ist der Bewerber damit einverstanden, muss er diesen Passus anhaken und unterschreiben. Der Beschwerdeführer habe zwar die Karten noch nicht ausgefüllt, jedoch habe es eine mündliche Rücksprache gegeben, dass das Profil anderen Kunden vorgestellt werden dürfe. Man habe das Profil nicht gelöscht, sondern nur gesperrt, weil es möglich sei, dass ein Bewerber noch Ansprüche auf Schadensersatz oder Entschädigung nach dem Allgemeinen Gleichbehandlungsgesetz geltend machen könnte. Dafür benötige man die Daten gegebenenfalls noch. Systemseitig sei an die fehlende Datenschutzerklärung erinnert worden, um bei Nichtvorlage die notwendige Löschung vornehmen zu können. Das Zeitarbeitsunternehmen wurde gefragt, ob es eine Dokumentation zu der mündlichen Rücksprache mit dem Bewerber gegeben habe. Das Unternehmen teilte mit, dass die mündliche Absprache im EDV-System dokumentiert worden sei. Aufgrund dieser Dokumentation werde eine systemseitig automatisierte Erinnerung an den Bewerber erzeugt, wenn zwischenzeitlich keine unterzeichnete Datenschutzerklärung eingegangen sei, um der zuvor mündlich getroffenen Vereinbarung eine schriftliche Grundlage zu geben. Der Beschwerdeführer habe diese Benachrichtigung erhalten, was zu Irritationen bei ihm geführt habe.

Nach § 4a Bundesdatenschutzgesetz (BDSG) bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das BDSG sieht danach nicht vor, dass die Einwilligung notwendigerweise schriftlich abgegeben wird. Wird eine andere Form gewählt, insbesondere die mündliche Einwilligung, gibt es, wie auch der vorliegende Fall zeigt, in der Praxis immer wieder Nachweisprobleme. Zwar schließt das Gesetz die Möglichkeit der mündlichen Einwilligung nicht aus, sie sollte aber wegen der mit ihr verbundenen Nachweisprobleme auf wenige Ausnahmefälle beschränkt werden. Hier hatte die möglicherweise mündlich erteilte Einwilligung zur Folge, dass andere Arbeitgeber erfuhren, dass eine bestimmte Person eine neue Arbeitsstelle sucht. Dabei ist es nicht ausgeschlossen, dass sich unter diesen Unternehmen auch der derzeitige Arbeitgeber eines Bewerbers befindet. Da mit einer derartigen Veröffentlichung unter Umständen weitreichende Folgen für den Betroffenen verbunden sind, hält der TLfDI in diesem Fall eine schriftliche Einwilligung für zwingend erforderlich. Dies hat er dem Zeitarbeitsunternehmen mitgeteilt. Das Zeitarbeitsunternehmen

teilte mit, dies sei im Nachhinein auch versucht worden, denn eine mündliche Absprache werde im EDV-System dokumentiert. Aufgrund dieser Dokumentation werde eine automatisierte Erinnerung an den Bewerber erzeugt, wenn keine unterzeichnete Datenschutzerklärung vorliege. Leider erfolgte diese automatische Ansprache erst, nachdem die Bewerbung bereits zurückgezogen worden war.

Wenn nach einem Löschbegehren der Bewerber im System gesperrt wird, ist unter Berücksichtigung der von der Zeitarbeitsfirma angeführten Gründe dagegen grundsätzlich nichts einzuwenden. Allerdings muss, wenn ein Bewerber seine Bewerbung zurückzieht, davon abgesehen werden, ihm weitere Angebote zukommen zu lassen. Die datenschutzrechtliche Prüfung hinsichtlich des Inhalts der veröffentlichten Bewerbung ist noch nicht abgeschlossen.

Vorsicht bei telefonischen Einwilligungen, die erhebliche datenschutzrechtliche Eingriffe nach sich ziehen. Insbesondere bei Eilbedürftigkeit kann man unter Umständen von einer Schriftlichkeit der Einwilligungserklärung absehen. Wenn mit einer Einwilligung weitreichende Folgen für den Betroffenen verbunden sind, sollte immer eine schriftlich erteilte Einwilligung vorliegen.

7.22 Kontrolle in einem Logistik-Unternehmen

Im Berichtszeitraum kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Logistikunternehmen. Ihm war zur Kenntnis gekommen, dass Leistungsdaten einzelner Arbeitnehmer aus den Logistikdaten zur Leistungskontrolle verwendet worden sein sollen.

Aufgrund der Komplexität der Datenverarbeitung dauerte die Kontrolle einige Zeit an. Das Unternehmen war äußerst kooperativ und unterstützte den TLfDI in all seinen Tätigkeiten vor Ort. So konnte der gesamte Logistikprozess begutachtet und Datenflüsse konnten nachvollzogen werden.

Im Ergebnis konnte festgestellt werden, dass der initiale Vorwurf wohl das Fehlverhalten einer einzelnen Führungskraft im unteren Managementbereich betraf und nicht systematisch Logistikdaten zur Leistungsüberwachung von Arbeitnehmern durch das Logistikunternehmen ausgewertet wurden.

Dennoch hat der TLfDI im Laufe seiner Kontrolle Mängel in der Datenverarbeitung aufgedeckt, die aber vom Unternehmen so schnell als möglich beseitigt wurden.

Im ganz überwiegenden Teil begründeten sich diese in der technischen Umsetzung von Datenflüssen und -verarbeitung im Logistikprozess. Bei jedem Logistikprozess, an dem Menschen beteiligt sind, entstehen personenbezogene Daten. Sobald zum Beispiel ein Arbeitnehmer einen Gegenstand in das Warensystem einordnet, wird dieser Umstand im System vermerkt. Während dies vordergründig ein systembezogenes Datum ist, lässt sich daraus natürlich auch eine Aussage über die Tätigkeit des Arbeitnehmers ableiten. Wenn dessen Tätigkeit darin besteht, regelmäßig Waren in die Warenwirtschaft einzupflegen, lässt sich hieraus eine sehr detaillierte Aussage über die Leistung des einzelnen Arbeitnehmers treffen. Insbesondere, weil man diese Daten mit denen anderer Arbeitnehmer, die eine vergleichbare Tätigkeit ausüben, vergleichen kann.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten nur dann erlaubt, wenn ein Gesetz diese Verarbeitung erlaubt oder anordnet oder der Betroffene in die Verarbeitung eingewilligt hat.

Einwilligungen lagen hier nicht vor. Da es sich um Daten über Arbeitnehmer handelt, ist einzige einschlägige Norm, die einen Umgang mit diesen Daten erlaubt, § 32 Abs. 1 Satz 1 BDSG. Hier hat der Gesetzgeber abschließend geregelt, wann eine Verarbeitung dieser Daten erlaubt ist. Dies ist dann der Fall, wenn der Umgang, also die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Eine darüber hinausgehende Berechtigung, Arbeitnehmerdaten zu verarbeiten besteht nur in Fällen von begründeten, dokumentierten Verdachtsfällen zu Straftaten gegenüber einzelnen Arbeitnehmern oder einer eng begrenzten Gruppe an Arbeitnehmern, § 32 Abs. 1 Satz 2 BDSG.

Die von oben erwähnte Führungskraft vorgenommene Leistungskontrolle war von der Verarbeitungsbefugnis, die sich aus § 32 Abs. 1 Satz 1 BDSG ergibt, nicht gedeckt, da sie für die Durchführung des Arbeitsverhältnisses nicht erforderlich war. Die Kontrolle über die Tätigkeit der Arbeitnehmer und deren Recht auf informationelle Selbstbestimmung sind zwei Interessen, die bei der Bewertung der Erforderlichkeit der Datenverarbeitung gegeneinander abgewogen werden müssen. Dabei ist auf der einen Seite das Interesse und

auch das Recht des Arbeitgebers zu berücksichtigen, die Leistung des einzelnen Arbeitnehmers bewerten zu können. Dies ist auch selbstverständlich, da es sich bei der konkreten Arbeitsleistung des Arbeitnehmers um die Primärleistung aus seinem Vertrag handelt. Wird diese nicht oder nur teilweise erfüllt, kann dies dazu führen, dass der Arbeitnehmer seinen Anspruch auf das Arbeitsentgelt ganz oder teilweise verliert. Der Arbeitgeber muss in der Lage sein, dieses Gegenseitigkeitsverhältnis von Ansprüchen prüfen zu können.

Andererseits darf, auch um dem informationellen Selbstbestimmungsrecht des Arbeitnehmers gerecht zu werden, kein „gläserner Arbeitnehmer“ entstehen. Diese Abwägung ist im Einzelfall sehr schwierig. Vorliegend war dies jedoch einfach, da jedenfalls dann die Interessen des Arbeitnehmers überwiegen, wenn der Arbeitgeber – oder wie hier eine einzelne Person – ein annähernd lückenloses Tätigkeits- und Bewegungsprofil des Arbeitnehmers erstellt.

Nun kann das einzelne Fehlverhalten einer Person nicht in jedem Fall auch dem Logistikunternehmen zugeordnet werden, so war dies auch hier. Die einzelne Person selber war leider nicht mehr ermittelbar, weswegen der TLfDI gegen diese nicht vorgehen konnte.

Allerdings muss ein Unternehmen seine Prozesse so gestalten, dass solch ein Fehlverhalten nicht möglich ist. Der beste Weg hierfür ist, den Zugriff von Daten so zu beschränken, dass jeder nur den Teil zu sehen bekommt, den er braucht, und die Daten, sobald ein Personenbezug nicht mehr notwendig ist, zu anonymisieren, also den Personenbezug zu entfernen. Diesen Weg hat das Unternehmen auf Anraten des TLfDI eingeschlagen und sein Logistiksystem insoweit überarbeitet.

Auch wenn die Verarbeitung von (auch) personenbezogenen Daten nicht der primäre Zweck einer Datenverarbeitung ist, müssen dabei das Datenschutzrecht und seine Vorschriften beachtet werden. Auch sind solche Systeme immer so zu gestalten, dass ein Zugriff auf Daten nur durch Personen erfolgt, die diese unbedingt benötigen und zu diesem Zweck auch verwenden dürfen. Werden Daten längerfristig benötigt, um Verarbeitungsschritte zu optimieren oder Fehler zu identifizieren, sind die Daten so früh wie möglich vom Personenbezug zu befreien.

Ortsnetzzrufnummer ist über die Bundesnetzagentur jedoch nicht möglich, da diese über derartige Informationen nicht selbst verfügt. Die Bundesnetzagentur vergibt lediglich sog. Rufnummernblöcke an Netzbetreiber, die daraufhin die einzelnen Rufnummern eigenverantwortlich an die Endkunden ausgeben. Diesen Auskunftsanspruch gegen die Bundesnetzagentur, der in § 66i Abs. 1 des Telekommunikationsgesetzes (TKG) enthalten ist, kann jeder, der ein berechtigtes Interesse hat, geltend machen und in Textform von der Bundesnetzagentur Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der eine Nummer von der Bundesnetzagentur zugeteilt bekommen hat.

§ 66i Abs. 3 TKG enthält auch einen Auskunftsanspruch gegen Dritte. Hiernach kann jeder, der ein berechtigtes Interesse daran hat, von demjenigen, dem von der Bundesnetzagentur Rufnummern zum Beispiel für Massenverkehrsdienste (0)137, Neuartige Dienste (0)12 oder Kurzwahldienste zugeteilt sind, unentgeltlich Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der über eine dieser Rufnummern Dienstleistungen anbietet, oder die Mitteilung verlangen, an wen die Rufnummer gemäß § 46 TKG übertragen wurde. Bei Kurzwahlnummern, die nicht von der Bundesnetzagentur zugeteilt wurden, besteht der Anspruch sogar gegenüber demjenigen, in dessen Netz die Kurzwahlnummer geschaltet ist. Im Falle des Beschwerdeführers handelte es sich um eine Ortsnetzzrufnummer. Diese werden nicht von der Bundesnetzagentur vergeben, sondern vom jeweiligen Netzbetreiber. Der Beschwerdeführer kann sich in diesem Fall an den Netzbetreiber wenden, den die Bundesnetzagentur mitgeteilt hat, um den Inhaber einer bestimmten Ortsnetzzrufnummer in Erfahrung zu bringen. Diese Anfrage ist jedoch nicht immer erfolgreich, da hinsichtlich der Ortsnetzzrufnummern der Anspruch aus § 66i Abs. 3 TKG gegen das jeweilige Telekommunikationsunternehmen nicht wie bei den Rufnummernbereichen (0)137 für Massenverkehrsdienste, (0)12 für Neuartige Dienste oder bei Kurzwahldiensten gegeben ist. Auch kann der Netzbetreiber aus vertraglichen oder datenschutzrechtlichen Gründen an einer Auskunft über seine Kunden gehindert sein. Dem Beschwerdeführer wurde durch die Anfrage des TLfDI bei der Bundesnetzagentur die Möglichkeit gegeben, beim Netzbetreiber hinsichtlich der ihn mit Werbeanrufen belästigenden Rufnummer eine Auskunft über den Namen und die ladungsfähige Anschrift zu erhalten.

Gegen lästige und aufdringliche Telefonwerbung kann die Hilfe der Bundesnetzagentur auch direkt vom Bürger selbst gemäß § 66i Abs. 3 TKG in Anspruch genommen werden (<https://www.bundesnetzagentur.de/ortsnetz>). Wenn der Netzbetreiber gefunden ist, kann eine Anfrage an diesen gestellt werden, um heraus zu finden, wer sich hinter einer bestimmten Rufnummer verbirgt, um mit diesem Wissen weitere Schritte einleiten zu können.



8.2 Auch Werbe-E-Mails entgehen dem Datenschutz nicht

Wer kennt das nicht: Bei Onlinebestellungen werden in der Regel vom Käufer sämtliche Angaben zu seiner Person verlangt; wie z. B. seine Adressdaten und/oder E-Mail-Adresse. Doch was passiert dann mit den Daten und wofür werden sie genutzt?

Ein typischer Fall ereignete sich bei einem Käufer eines Bürofachhandels. Der Käufer bestellte dort online und erhielt im Anschluss des Kaufes weitere E-Mails mit werblichem Inhalt. Er wandte sich daraufhin an das Unternehmen und bat nach § 34 Bundesdatenschutzgesetz (BDSG) um Auskunft, welche Daten letztendlich über ihn gespeichert sind, welche Daten evtl. an Dritte weitergegeben werden und forderte die Löschung seiner Daten. Da er nach seiner Aussage keine Antwort vom Bürofachhandel erhielt, wandte er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte sein Anliegen mit.

Nach § 34 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung. Vor diesem Hintergrund wandte sich der TLfDI an den Bürofachhandel und forderte diesen auf, dem Auskunftersuchen nach § 34 Abs. 1 BDSG gegenüber dem betroffenen Käufer nachzukommen. Der Bürofachhandel reagierte und teilte u. a. mit, dass er bereits beim ersten Schreiben vom Käufer auf dessen Anliegen rea-

giert habe, er die geforderte Auskunft gegeben habe und legte das anhand der Ausgangsschreiben dem TLfDI vor. Auch auf Nachfrage bei dem betroffenen Käufer stellte sich heraus, dass er mit der Auskunft zufriedengestellt wurde und das nun endlich seine personenbezogenen Daten, die beim Bürofachhandel gespeichert waren, gelöscht wurden. Er sollte keine weiteren Werbe-E-Mails erhalten.

Nach § 34 BDSG besteht eine gesetzliche Auskunftspflicht über gespeicherte Daten eines Betroffenen bei einer verantwortlichen Stelle. Jeder Betroffene kann sich auf Grundlage des § 34 BDSG an verantwortliche Stellen wenden und Auskunft über seine gespeicherten Daten verlangen. Erhält der Betroffene keine Auskunft, kann er sich jederzeit an den TLfDI wenden.



Lupe Schufa - ©JiSign / Fotolia.com

9 Auskunftfeien

9.1 Verhindert die SCHUFA Dispositionskredit?

Ein Abgeordneter des Thüringer Landtags bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft zur Frage der Löschung von Einträgen bei der Schufa. Der Abgeordnete selbst hatte eine Anfrage eines Bürgers vorliegen, dem ein beantragter Dispositionskredit in geringer Höhe verwehrt worden war. Dies war möglicherweise auf eine Forderung zurückzuführen, die bereits getilgt war und auf die Eintragung der Privatinsolvenz, zu der bereits eine Restschuldbefreiung erteilt wurde.

Der TLfDI wies zunächst darauf hin, dass er für die Schufa Holding AG keine Zuständigkeit habe, weil sie ihren Sitz nicht in Thüringen hat. Zuständig ist für die SCHUFA die hessische Datenschutzaufsicht.

Unter dieser Prämisse führte der TLfDI in der Sache aus, dass § 28 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Zulässigkeitsvoraussetzungen für die Einmeldung von Forderungen aufzählt. Selbstverständlich besteht für den Betroffenen die Möglichkeit, nach § 34 Abs. 2 BDSG Auskünfte über die zu seiner Person gespeicherten

Daten bei der SCHUFA zu beantragen. Nach § 34 Abs. 8 BDSG ist die Auskunft unentgeltlich und kann vom Betroffenen einmal je Kalenderjahr verlangt werden. Sollte sich ergeben, dass noch Forderungen gespeichert sind, die bereits ausgeglichen sind, kann der Betroffene unter Umständen Löschung verlangen.

Die Erhebung und Verarbeitung der personenbezogenen Daten des Betroffenen durch die SCHUFA im Falle der Eröffnung einer Privatinsolvenz erfolgt in der Regel nach der Veröffentlichung in den Insolvenzbekanntmachungen als öffentlich zugängliche Quelle nach § 29 Abs. 1 Nummer 2 BDSG und liegt im Sinne des Gläubigerschutzes. Liegt bereits eine Restschuldbefreiung vor, kann auch diese veröffentlichte Entscheidung bei der SCHUFA gespeichert werden. Nach den Informationen auf der Internetseite der SCHUFA wird nach Erteilung der Restschuldbefreiung nach Ablauf eines Zeitraums von drei Jahren zum Jahresende dies im SCHUFA-Datenbestand gelöscht. Diese grundsätzliche Datenspeicherfrist kann aufgrund der Abwägung der Interessen der Wirtschaft zur Einschätzung eines geschäftlichen Risikos mit den Interessen des Betroffenen gerechtfertigt werden und ist datenschutzrechtlich nicht unzulässig.

Trotz der Restschuldbefreiung war demnach noch mit einer weiteren Speicherung zu rechnen. Kommt es in dieser Zeit zur Ablehnung eines beantragten Dispositionskredits, kann sich der Betroffene an die entsprechende Bank wenden und seine Belange vortragen. Die Entscheidung, einem Betroffenen einen Dispositionskredit einzuräumen oder zu versagen, unterliegt jedoch keiner datenschutzrechtlichen Bewertung.

Lehnt eine Thüringer Bank die Gewährung eines Dispositionskredits unter Hinweis auf Eintragungen bei der SCHUFA ab, kann sich der Betroffene durch eine Auskunft nach § 34 BDSG über die Eintragungen informieren und sich gegebenenfalls an die für die SCHUFA zuständige hessische Datenschutzaufsicht wenden. Die Entscheidung, einem Betroffenen einen Dispositionskredit einzuräumen oder zu versagen, unterliegt allerdings nicht der datenschutzrechtlichen Bewertung.

9.2 Überraschung: Ware nur nach Bonitätsabfrage

Im 2. Tätigkeitsbericht für den nicht-öffentlichen Bereich wurden unter Nummer 7.6 die Abläufe im Onlinehandel und die datenschutz-

rechtlichen Aspekte beim Onlineeinkauf dargestellt. Immer wieder gibt es Irritationen, wenn der Kauf unbemerkt für den Kunden eine Bonitätsabfrage bei einer Auskunft voraussetzt.

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem er versucht hatte, bei einem Thüringer Onlinehändler Ware im mittleren zweistelligen Wert zu bestellen und im Lastschriftverfahren zu bezahlen. Für ihn unerwartet wurde von ihm Vorkasse verlangt. Dies erklärte er sich damit, dass offenbar automatisch eine im „Kleingedruckten“, also in den Allgemeinen Geschäftsbedingungen (AGB), angesprochene Bonitätsabfrage bei einer Auskunft durchgeführt worden war, was er im Hinblick auf den doch relativ geringen Warenwert für unverhältnismäßig ansah. Seine Anfrage an das Onlineunternehmen, welche negativen Auskünfte denn vorlägen, war nur kurz und knapp beantwortet worden. Bei einer erstmaligen Bestellung behalte man sich unabhängig vom Warenwert das Recht auf Vorkasse vor. Schließlich habe er die AGB bestätigt, die auf diese Möglichkeit hinwiesen. Wegen der Einstufung seiner Bonität solle er sich bitte an die Auskunft wenden, denn hierzu speichere das Unternehmen keine Daten.

Der TLfDI teilte dem Betroffenen zu dem Problem der Verweisung an die Auskunft mit, dass sich bei einer datenschutzrechtlichen Prüfung bestätigt hatte, dass das Unternehmen tatsächlich eine eventuell eingeholte Auskunft über die Bonität nicht speichere und daher nur die Auskunft ihm Auskunft darüber erteilen könne, welche Bonitätswerte dort gespeichert werden. Weiterhin konnte vom TLfDI bei einer Kontrolle nicht festgestellt werden, dass das Unternehmen generell und automatisch unabhängig vom Vorliegen eines möglichen wirtschaftlichen Risikos Bonitätsabfragen vornimmt. Auf der Internetseite werden verschiedene Bezahlungsmöglichkeiten angeboten. Beim Kauf nach Vorkasse oder per Nachnahme bestehen für den Verkäufer der Ware keine wirtschaftlichen Risiken. Er erhält sicher Geld gegen Ware. Der Kauf auf Rechnung und das Lastschriftverfahren sind dagegen mit einer gewissen Unsicherheit behaftet, ob das Konto gedeckt ist oder ob der Kunde zahlungswillig und -fähig ist. Das Unternehmen muss sich nicht auf eine dieser „unsicheren“ Zahlungsarten einlassen, bei denen das Risiko besteht, dass der Kaufpreis möglicherweise nicht entrichtet wird und damit wirtschaftlicher Schaden entsteht. Dass der Verkäufer versucht, sein wirtschaftliches Risiko zu minimieren, muss akzeptiert werden. Dies darf er aber

nicht unbemerkt durch den Kunden durch eine Bonitätsabfrage als Datenerhebung über den Kunden tun.

Zieht die Auswahl einer unsicheren Zahlungsart eine Bonitätsabfrage bei einer Auskunft nach sich, muss dies der Käufer frühzeitig bei der Auswahl der Zahlungsart erkennen können. Um sich bewusst für eine Zahlungsart mit oder ohne Bonitätsauskunft entscheiden zu können, darf der Kunde nicht nur darauf verwiesen werden, es sei aus den umfangreichen Allgemeinen Geschäftsbedingungen zu entnehmen, dass Bonitätsabfragen grundsätzlich möglich sind. Im Falle der Auswahl einer unsicheren Zahlungsart bedarf es keiner Einwilligung des Betroffenen nach § 4a Bundesdatenschutzgesetz (BDSG) zur Auskunftabfrage, denn die Rechtsgrundlage für die Auskunftabfrage bildet § 28 Abs. 1 Nr. 2 BDSG. Danach ist eine Datenverarbeitung aufgrund der Erforderlichkeit zur Wahrung des berechtigten Interesses des Onlineverkäufers zulässig. Jedoch bedarf es zur Information für den Betroffenen der konkreten Angabe, in welchem Fall mit einer Bonitätsabfrage zu rechnen ist, damit er sich bewusst für eine Zahlungsart mit oder ohne Auskunftabfrage entscheiden kann. Aus Gründen der Transparenz und Klarheit hat sich das Onlineunternehmen bereit erklärt, neben der Auswahlmöglichkeit von sogenannten unsicheren Bezahlarten einen Hinweis aufzunehmen, dass dies die Bonität voraussetzt und damit eine Auskunftabfrage verbunden sein kann.

Das Vorgehen des Unternehmens, bei erstmaligen Bestellungen nur auf Vorkasse zu liefern, stieß im Übrigen ebenfalls nicht auf datenschutzrechtliche Bedenken, denn mit diesem Vorgehen sind keine weiteren Datenerhebungen und Verarbeitungen verbunden.

Bei der Auswahl der Zahlungsart muss der Käufer im Onlinehandel wissen, ob eine bestimmte Art eine Bonitätsabfrage bei einer Auskunft voraussetzt. Es ist kein Datenschutzproblem, wenn bei der ersten Bestellung eines Kunden das Unternehmen eine bestimmte sichere Zahlungsart verlangt, um sein wirtschaftliches Risiko zu begrenzen.

9.3 Schweigen eines Versandhandels

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Bürgers, der in einem großen Versandhandel in Thüringen eine Bestel-

lung getätigt hatte. Nachdem das Produkt dort aber wohl nicht mehr erhältlich gewesen ist, wurde seine Bestellung vom Versandunternehmen storniert und er darüber in Kenntnis gesetzt.

Daraufhin wollte der Bürger gerne wissen, welche Daten das Unternehmen über ihn speichert, und verlangte zudem, dass sein Kundenaccount, den er eigens für diese nicht ausgeführte Bestellung eingerichtet hatte, gelöscht wird. Er verlangte eine Auskunft gemäß § 34 Bundesdatenschutzgesetz (BDSG) über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft der Daten beziehen, den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden, und den Zweck der Speicherung, § 34 Abs. 1 Nr. 1 bis 3 BDSG. Als er nach Ablauf einer ausreichend bemessenen Frist keine Antwort vom Unternehmen erhalten hatte, schrieb er es erneut unter Fristsetzung an. Das Versandunternehmen reagierte allerdings überhaupt nicht auf dieses Auskunftsverlangen, auch nicht mit einer Negativauskunft. Diese wäre immer dann zu erteilen, wenn keine Daten mehr im Unternehmen vorliegen oder gespeichert werden. Aus diesem Grund wurde das Versandunternehmen seitens des TlfdI aufgefordert, eine entsprechende Auskunft gemäß § 34 BDSG an den Betroffenen zu erteilen, und es wurde mitgeteilt, dass der Account zu sperren und ggf. auch zu löschen ist, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Weiterhin wurde durch den TlfdI ein Auskunftsersuchen an das Unternehmen gerichtet, indem es aufgefordert wurde mitzuteilen, welche technischen und organisatorischen Maßnahmen es getroffen hat, um dafür Sorge zu tragen, dass ein Auskunftsersuchen gemäß § 34 BDSG umfassend an den Betroffenen beantwortet wird. Dem Auskunftsverlangen nach § 34 BDSG an den Betroffenen kam das Unternehmen dann auch nach. Es erklärte weiterhin durch seinen betrieblichen Datenschutzbeauftragten gegenüber dem TlfdI, künftig dafür Sorge zu tragen, dass alle Auskunftsverlangen direkt dem Datenschutzbeauftragten zugeleitet werden und nicht wie bisher an die Sachbearbeiter des Unternehmens, die diese nach eigenem Ermessen beantwortet haben oder eben auch nicht.

Das Auskunftsrecht des Betroffenen gem. § 34 BDSG ist von der verantwortlichen Stelle immer zu beachten. Die Auskunft muss sich dabei auf alle zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft der Daten beziehen, den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben wer-

den, und den Zweck der Speicherung beziehen, § 34 Abs. 1 Nr. 1 bis 3 BDSG. Für den Fall, dass eine verantwortliche Stelle keine Daten über den Betroffenen erhoben oder gespeichert hat, ist eine sog. Negativauskunft zu erteilen.



Stethoskop mit Gesundheitskarte auf Geldscheinen - © Zerbor / Fotolia.com

10 Gesundheit

10.1 Ansteckende Krankheiten sind Privatsphäre, oder nicht?

Anfang Februar 2016 erkundigte sich die Mitarbeiterin einer Betreuungseinrichtung danach, inwieweit die Mitarbeiter zu betreuende Schwerstkranke und deren Familien über nachgewiesene Keime (zum Beispiel MRSA) bei einer betreuten Person informieren dürfen. Hintergrund dieser Frage war der Schutz vor Infektionen für die weiteren Familien. Nach eigener Angabe traf die Einrichtung bei Keimbelastungen umfangreiche, hygienische Schutzmaßnahmen, die die Familie der betreuten Person einzuhalten hatte. Dennoch war es den Mitarbeitern wichtig, einen weitgehend normalen Aufenthalt zu ermöglichen und beispielsweise die Isolation der betroffenen Personen zu vermeiden. Die Einhaltung der Schutzmaßnahmen würde jedoch erschwert, wenn nicht alle potenziell Betroffenen über die Infektion informiert sind.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beantwortete die Fragen der Betreuungseinrichtung folgendermaßen: Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten an Dritte grundsätzlich nur übermittelt werden, wenn es eine Rechtsgrundlage hierfür gibt

oder der Betroffene eingewilligt hat. Bei der Frage, ob ein Befall mit multiresistenten Keimen vorliegt, handelt es sich um Angaben über die Gesundheit und damit um besondere Arten von Daten nach § 3 Abs. 9 BDSG. Diese Daten unterliegen einem besonderen gesetzlichen Schutz. Die Fälle, in denen die Übermittlung von Gesundheitsdaten zulässig ist, regelt § 28 Abs. 6 beziehungsweise Abs. 7 Satz 2 BDSG. In einer Betreuungseinrichtung ist davon auszugehen, dass die Mitteilung über den Befall mit multiresistenten Keimen an andere potenziell Betroffene zum Schutz ihrer Interessen notwendig ist. Hier werden Betreute behandelt, deren Immunabwehr u. U. sehr geschwächt ist. Für deren Familien ist es von existenzieller Bedeutung, die Ansteckungsgefahr zu kennen, denn nur dann können sie sich und vor allem ihre betreuten Familienangehörigen auch innerhalb der Einrichtung hinreichend schützen. Nach § 28 Abs. 7 Satz 2 und Satz 2 BDSG richtet sich die Zulässigkeit der Verarbeitung und Nutzung von Daten zur Gesundheitsvorsorge, medizinischen Diagnostik, Gesundheitsversorgung oder -behandlung nach den für ärztliches Personal geltenden Geheimhaltungspflichten (ärztliches Personal oder sonstige Personen). Die Übermittlung stellt einen Fall der Verarbeitung von Daten dar. Den Maßstab für die Zulässigkeit stellt § 203 Strafgesetzbuch (StGB) mit seiner Wertung zur Geheimhaltungspflicht dar. Danach darf ein Geheimnis, das einem Arzt oder medizinischem Personal anvertraut oder bekannt gemacht wurde durch diese nur offenbart werden, wenn sie dazu befugt sind. Dies kann sich aus einer Einwilligung (Schweigepflichtentbindung) oder einer Offenbarungsbefugnis ergeben. Gemäß § 34 StGB kann sich die Befugnis auch aus einem sogenannten rechtfertigenden Notstand ergeben, beispielsweise dem Schutz von Rechtsgütern Dritter. Dies wäre der Fall, wenn ein Patient sich trotz der Belehrung des Arztes weigert, gefährdete Personen über eine bestehende Infektionsgefahr aufzuklären (Fischer, Kommentar zum StGB, 63. Aufl. Rn. 47 zu § 203 m. w. N.). Somit ist die Information der Familienangehörigen über die Infektion einer betreuten Person mit multiresistenten Keimen nach § 28 Abs. 7 Satz 2 BDSG zulässig. Um die Akzeptanz dieser Information zu erhöhen, empfahl der TLfDI der Einrichtung, alle Beteiligten über die Gründe der Weitergabe in Kenntnis zu setzen und die Einrichtung sollte versuchen, die mit den multiresistenten Keimen infizierten Betroffenen bzw. deren Familien zur Einwilligung in die Weitergabe der Daten zu bewegen.

Besteht eine tatsächliche Gefahr für Leib und Leben von Personen, kann die Übermittlung von Gesundheitsdaten an gefährdete Personen nach § 34 StGB im Einzelfall gerechtfertigt sein, auch wenn sie mangels gesetzlicher Übermittlungsbefugnis oder Einwilligung der datenschutzrechtlich Betroffenen rechtswidrig ist.

10.2 Antworten zum betriebsärztlichen Datenschutz

Im Januar 2016 bat der Arbeitsmedizinische Dienst (AMD) eines Klinikums in Jena den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um datenschutzrechtliche Auskunft zu Dokumentationen von Betriebsärzten. Der AMD betreut als Dienstleister Firmen in und um Jena betriebsärztlich. Infolge der Beendigung des Betreuungsvertrages mit einer Firma und dem Wechsel des externen Betriebsarztes ergab sich die Frage, inwiefern Betriebsarzt dokumentationen an den betriebsärztlichen Nachfolger übergeben werden dürfen. Bei der eigenen Recherche hatte der AMD hierzu teilweise verschiedene Festlegungen gefunden.

Der Sachverhalt wurde vom AMD Jena folgendermaßen dargestellt: Vor dem Ausscheiden des alten Betriebsarztes hatte die Firma ihre Mitarbeiter in einem Rundschreiben über den betriebsärztlichen Wechsel informiert und ihnen die Möglichkeit gegeben, der Aktenübergabe zu widersprechen. Nachdem kein Widerspruch ergangen war, forderte die Firma den ausscheidenden Betriebsarzt auf, dem neuen Betriebsarzt sämtliche Akten zu übergeben. Während der Aktenübergabe stellte sich heraus, dass der neue Betriebsarzt keine Möglichkeit hatte, die Akten in seinen Räumen aufzubewahren. Da das Unternehmen für die Datenverarbeitung durch den Betriebsarzt verantwortlich ist, sollten die Akten bei der Firma selbst aufbewahrt werden, vorausgesetzt, die Firma als Arbeitgeber kann selbst keinen Einblick in die Unterlagen nehmen. Die Akten sollten nach aktiven und inaktiven Mitarbeitern sortiert werden. Akten von aktiven Mitarbeitern sollten mit Zugriffsmöglichkeit des Betriebsarztes verschlossen und Akten von nicht mehr im Dienst befindlichen Mitarbeitern verschlossen und verplombt im Archiv des Betriebes aufbewahrt werden. Die Kisten mit den Akten der aktiven Mitarbeiter sollten vom betrieblichen Datenschutzbeauftragten direkt an den neuen Betriebsarzt übergeben werden. Alternativ wurde vom Klinikum auch eine direkte Übergabe dieses Aktenteils an den neuen

Betriebsarzt erwogen. Es sollte ein datenschutzkonformes Übergabeprotokoll mit der Anzahl der Akten von aktiven und inaktiven Mitarbeitern, namentlich sortiert, erstellt werden.

Im Hinblick auf dieses Vorgehen richtete der AMD an den TLfDI mehrere Fragen: Ist die geplante Archivierung der inaktiven Akten im Betrieb datenschutzrechtlich in Ordnung? Müssen Akten getrennt werden, wenn sie Daten enthalten, die außerhalb der arbeitsmedizinischen Vorsorge oder des Arbeitssicherheitsgesetzes erhoben wurden? Sollten nur objektive Befunde (beispielsweise Labordaten und Impftiter-Daten zu Antikörpern im Blut) übergeben werden? Ist es datenschutzkonform, wenn Akten von inaktiven, nicht mehr angestellten Mitarbeitern übergeben werden? Falls der neue Betriebsarzt gegen das Datenschutzrecht verstößt und ohne Zustimmung der Mitarbeiter Einsicht in eine Akte nimmt, kann dann auch der scheidende Betriebsarzt haftbar gemacht werden, da er die Akte abgegeben hat? Muss für die Aktenübergabe ein Widerspruchsverfahren durchgeführt werden? Bedarf die Akteneinsicht der ausdrücklichen Zustimmung des Mitarbeiters und müssen diese Akten bis zur Freigabe einzeln verschlossen verpackt sein?

Der TLfDI gab für die Übergabe der Dokumentation folgende Hinweise:

Grundlage für die Tätigkeit der Betriebsärzte sind das Arbeitssicherheitsgesetz (ASiG) und die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV). Nach § 3 ASiG ist es die Aufgabe des Betriebsarztes, den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu beraten und zu unterstützen. Auf dieser Grundlage erfolgt die Untersuchung von Arbeitnehmerinnen und Arbeitnehmern. Die betriebsärztliche Dokumentation beinhaltet sowohl arbeitnehmerbezogene individuelle medizinische als auch arbeitgeberbezogene Arbeitsplatzaspekte. Der Betriebsarzt unterliegt der ärztlichen Schweigepflicht und ist nach § 8 Abs. 1 ASiG gegenüber dem Arbeitgeber unabhängig. Daher muss ausgeschlossen werden, dass der Arbeitgeber Zugriff auf die Patientenkartei erhält. Dieser Ausschluss ist durch das beschriebene Vorgehen erfüllt. Akten von nicht mehr im Arbeitsverhältnis stehenden Mitarbeitern können beim Arbeitgeber gelagert werden, jedoch hat der frühere Betriebsarzt gemäß § 10 Abs. 4 Satz 1 der Berufsordnung der Landesärztekammer Thüringen dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Der übernehmende Betriebsarzt muss diese Aufzeichnungen unter Verschluss halten und darf sie

nur mit Einwilligung des Patienten einsehen. Danach darf selbst der Datenschutzbeauftragte des Unternehmens keinen Zugriff auf diese Daten haben.

Nach der ArbMedVV muss der Arbeitgeber Pflicht- und Angebotsvorsorgen sowie Wunschvorsorgeuntersuchungen anbieten. Die Arbeitnehmer sind nur verpflichtet, an der Pflichtvorsorge mit Beratungsgespräch und Arbeitsanamnese teilzunehmen; weitergehende Untersuchungen können sie gemäß § 2 Abs. 1 Nr. 3 ArbMedVV ablehnen. Die strikte Trennung zwischen Vorsorge zur Gesundheit des Arbeitnehmers und Eignungsuntersuchungen für Zwecke des Arbeitgebers sollte sich auch in der Dokumentation des Betriebsarztes widerspiegeln. Insofern müssen Angaben zu Eignungsuntersuchungen getrennt verwahrt werden. Bei einem Wechsel des Betriebsarztes darf der Nachfolger nur mit persönlicher Einwilligung des Betroffenen auf diese Informationen zugreifen.

Arbeitnehmer können die Einsichtnahme durch den neuen Betriebsarzt in die gesundheitsbezogene Dokumentation früherer Untersuchungen ablehnen (§ 10 Abs. 4 Satz 2 Berufsordnung der Landesärztekammer Thüringen). Diese Unterlagen dürfen nicht vom neuen Betriebsarzt beizugezogen werden; sie müssen bis zur Löschungsfrist besonders geschützt im Betrieb aufbewahrt werden. Der Nachfolger darf nur mit persönlicher Einwilligung des Betroffenen Zugriff auf diese Informationen nehmen. Der neue Betriebsarzt muss jedoch auf die für seine Arbeit notwendigen Stammdaten seines Vorgängers nach dem ASiG und der ArbMedVV Zugriff haben, d. h. auf die Angaben, die gegenüber dem Arbeitgeber zu attestieren sind: Art und Datum der Vorsorge und Datum der nächsten Vorsorge. Auch auf die vom Betriebsarzt erstellte Arbeitsplatzbeschreibung muss der Nachfolger zugreifen können.

Der Arbeitnehmer muss einer Übergabe der Betriebsarzt-dokumentation an einen neuen Betriebsarzt im Vorfeld nicht zustimmen. Aus Transparenzgründen müssen die Mitarbeiter jedoch rechtzeitig und umfassend über den geplanten Wechsel des Betriebsarztes informiert werden. Für die Datenverarbeitung durch den Betriebsarzt ist gemäß § 2 Abs. 2 Satz 1 ASiG das Unternehmen verantwortlich, nicht der Betriebsarzt. Wenn der scheidende Betriebsarzt bei der Übergabe der Akten die datenschutzrechtlichen Vorgaben einhält, kann er durch die Aufsichtsbehörde nicht für Datenschutzverstöße des neuen Betriebsarztes herangezogen werden.

Grundlage für die Tätigkeit von Betriebsärzten sind das Arbeitssicherheitsgesetz (ASiG) und die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV). Für die Datenverarbeitung durch den Betriebsarzt ist das beauftragende Unternehmen verantwortlich, nicht der Betriebsarzt. Wenn ein Unternehmen den externen Betriebsarzt wechselt, muss die betriebsärztliche Dokumentation unter Einhaltung bestimmter datenschutzrechtlicher Regelungen an den Nachfolger übergeben werden. Aus Transparenzgründen sind die Mitarbeiter im Vorfeld über den Wechsel zu informieren. Der neue Betriebsarzt hat, damit er seine Aufgaben nach dem ASiG erfüllen kann, auch ohne Einwilligung der Beschäftigten regelmäßig nur Zugriff auf die Stammdaten des Vorgängers, die gegenüber dem Arbeitgeber zu attestieren sind, wie beispielsweise Art und Datum der Vorsorge und Termin der nächsten Vorsorge sowie die Arbeitsplatzbeschreibung. Dies ist nicht direkt gesetzlich geregelt, sondern ergibt sich aus der im ASiG festgelegten Aufgabe des Betriebsarztes. Nach § 3 ASiG hat der Betriebsarzt den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu beraten und zu unterstützen. Die Einsichtnahme in die gesundheitsbezogene Dokumentation früherer Untersuchungen können die Arbeitnehmer ablehnen. Diese Unterlagen sind nach § 15 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz zu sperren und bis zum Ablauf der Lösungsfrist besonders geschützt im Betrieb aufzubewahren.

10.3 Der Apotheker als Ermittlungshelfer der Polizei?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage einer Apotheke, ob sie Kundendaten an die Polizei zur Strafverfolgung herausgeben kann. Hintergrund war die Anfrage einer Landespolizeiinspektion, die wegen eines Verkehrsunfalls ermittelte. Die Polizeibehörde war auf der Suche nach dem Unfallverursacher, der sich unerlaubt vom Tatort entfernt hatte. Laut der Polizei kämen hierfür drei Kunden der Apotheke in Frage, weshalb um eine namentliche Bekanntgabe gebeten wurde.

Die Apotheke erfasst Daten für kundenorientierte Zwecke nur nach zuvor erteilter Einwilligung der betroffenen Person. Ein anderer Weg der Ermittlung von Kundendaten wäre, nach Auskunft der Apotheke, durch Zuordnung von anonymisierten Rezeptdaten möglich. Die

Erhebung und Speicherung der personenbezogenen Daten durch die Apotheke unterliegt jedoch dem Zweckbindungsgebot. Nach § 28 Abs. 1 Nr. 1 BDSG sind die Erhebung, Speicherung, Veränderung oder Übermittlung personenbezogener Daten sowie ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Fraglich ist also, ob die Apotheke die Daten zweckentfremden kann und zur Ermittlung einer Straftat an die Polizeibehörden übermitteln darf.

Die Polizei ist nach § 163 Abs. 1 Strafprozessordnung (StPO) dazu verpflichtet, Straftaten zu erforschen. Zu diesem Zweck ist sie befugt, Ermittlungen jeder Art vorzunehmen, worunter auch ein Auskunftersuchen an ein privates Unternehmen fällt. Allerdings kann die Datenauskunft nicht verlangt werden, denn dem privaten Unternehmen wird keine Mitwirkungspflicht auferlegt. Nach § 28 Abs. 2 Nr. 2b BDSG ist die Übermittlung oder Nutzung der Daten zu einem anderen Zweck zulässig, soweit es zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Allerdings verlangt auch diese Norm keine Pflicht der Übermittlung.

Allerdings könnte die Staatsanwaltschaft oder das Gericht eine Pflicht der Mitteilung herbeiwirken (Vorladung des Apothekers als Zeugen nach § 161a StPO oder Beschlagnahmung der Unterlagen §§ 95,98 StPO).

In dem vorliegenden Fall kann sich die Apotheke jedoch auf ihr Zeugnisverweigerungsrecht gemäß § 53 Abs. 1 Nr. 3 StPO berufen. Demnach sind Apotheker dazu berechtigt, über das, was ihnen in dieser Eigenschaft anvertraut oder bekannt geworden ist, das Zeugnis zu verweigern. Laut Kommentarliteratur zählt zu dem geschützten Bereich auch der Name des Patienten (Radke/Hohmann, § 53, Rn. 19). Dies ist nach Ansicht des TLfDI auch anwendbar auf den Apotheken – „Kunden“.

Eventuell könnte sich der Apotheker sogar nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) strafbar machen, wenn er die Daten herausgibt. Gemäß § 203 Abs. 1 Nr. 1 StGB macht sich strafbar, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Le-

bensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Apotheker anvertraut worden oder sonst bekannt geworden ist.

Der Apotheker kann sich auf sein Zeugnisverweigerungsrecht berufen, das sich auf die Tatsachen erstreckt, die dem Apotheker als Zeuge bei der Berufsausübung anvertraut oder bekannt geworden sind, wozu auch die Namen seiner Kunden zählen. Somit muss der Apotheker der Bitte der Polizei nicht Folge leisten.

Nach § 28 Abs. 1 BDSG ist das Erheben von Daten zum Durchführen von Rechtsgeschäften zulässig. Jedoch muss der Zweck der Verarbeitung oder Nutzung von personenbezogenen Daten zuvor definiert werden. Eine zweckentfremdete Nutzung und Übermittlung von Daten ist nur innerhalb der genannten Ausnahmen des § 28 Abs. 2 BDSG erlaubt. Berufsgeheimnisträger, zu denen unter anderem auch Apotheker gehören, haben das Recht auf Zeugnisverweigerung, um Ihrer Pflicht, kein fremdes Geheimnis zu verraten, gerecht zu werden (Verbot aus § 203 StGB).

10.4 Datenschutz bald verschreibungspflichtig?

Eine Mitinhaberin einer Apotheke wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Anliegen, dass sie den Verdacht hat, ihre ehemalige Mitarbeiterin habe Patientendaten aus der Kundenkartei gestohlen. Die ehemalige Mitarbeiterin arbeite jetzt bei einem neu eröffneten Sanitätshaus. Seit dem wurden Kunden der Apotheke vom Sanitätshaus kontaktiert, um für dessen Produkte und Leistungen zu werben. Viele Kunden waren über die Werbeanrufe empört und konnten es nicht nachvollziehen, wie das Sanitätshaus an die nicht-öffentlich zugänglichen Telefonnummern gekommen sei. Des Weiteren bestand der Verdacht, dass ausgestellte Rezepte der Apotheke kopiert worden waren, da das Sanitätshaus gezielt Anrufe an die Betroffenen getätigt und an den Ablauf des Rezepts erinnert hatte.

Der TLfDI hatte im Rahmen seiner aufsichtsbehördlichen Tätigkeit eine Vor-Ort-Kontrolle bei dem genannten Sanitätshaus veranlasst. Die mit der Kontrolle beauftragten Personen des TLfDI sind nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) berechtigt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben er-

forderlich ist, während der Betriebs- und Geschäftszeiten die Grundstücke und Geschäftsräume der verantwortlichen Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Im Vorfeld der Kontrolle wurden von der Beschwerdeführerin Nachweise geliefert, die dazu dienen sollten, dass Patientendaten von der ehemaligen Mitarbeiterin gestohlen wurden. Bei der Kontrolle wurden diese Patientendaten abgeglichen. Das Sanitätshaus wies glaubhaft mit seinen Unterlagen nach, dass die Patientendaten selbst erhoben wurden. Die einzige Neukundengewinnung wurde über Werbeanzeigen in der Tagespresse sowie über Informationsmaterial geschaltet; gezielte Anrufe wurden nicht getätigt. Auch die in Rede stehenden Patientendaten von verstorbenen Patienten der Apotheke konnten bei der Sichtung der Unterlagen nicht nachgewiesen werden. Somit konnte der TLfDI keinen Datendiebstahl der Patientendaten und damit keinen Datenschutzverstoß feststellen.

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit nach § 42 Thüringer Datenschutzgesetz (ThürDSG) führt der TLfDI regelmäßig Unternehmenskontrollen oder Kontrollen, bei denen der Verdacht eines Verstoßes gegen die Vorschriften des Bundesdatenschutzgesetzes vorliegt, durch. Hierzu ist der TLfDI nach § 38 Abs. 4 BDSG berechtigt. Im oben genannten Fall konnte allerdings kein datenschutzrechtlicher Verstoß festgestellt werden.

10.5 Patientendaten unverschlüsselt im IT-Dschungel

Der Landesbeauftragte für den Datenschutz von Sachsen-Anhalt (LfD Sachsen-Anhalt) leitete die Anfrage eines IT-Unternehmens aus seinem Bundesland an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter. Die Anfrage des Unternehmens bezog sich auf die Patientensoftware einer Firma aus Thüringen.

Das IT-Unternehmen gab an, eine ambulante Tagespflege zu betreuen. Dieses Pflegeunternehmen setzte die Software einer Thüringer Firma ein. Die Mitarbeiter des Pflegedienstes sollten mit mobilen Endgeräten (Smartphones bzw. Tablets) ausgestattet werden. Um auf den zentralen Server zugreifen zu können, sollte das betreuende IT-Unternehmen die Firewall entsprechend einrichten. Die freizugebenden Schnittstellen erschienen dem beauftragten IT-Unternehmen nicht sicher. Das IT-Unternehmen wollte jedoch nicht für Datenlecks

haftbar gemacht werden und kritisierte im Hinblick darauf die eingesetzte Software. Dem sachsen-anhaltischen LfD lagen keine Informationen zur genutzten Software des Pflegedienstes vor. Das IT-Unternehmen bat darum, den Thüringer Software-Hersteller auf seine Verantwortung für den Datenschutz hinzuweisen.

Der TLfDI bat das IT-Unternehmen zunächst um eine genaue Darlegung der technischen und organisatorischen Gegebenheiten des Pflegedienstes. Diese wurden folgendermaßen beschrieben: Der Pflegedienst betrieb in Sachsen-Anhalt einen Server, auf dem das Programm der Thüringer Software-Firma lief. Auf diesen Server sollten die Mitarbeiter über Smartphones und Laptops zugreifen können. Genauere Zugriffsmethoden konnten durch das IT-Unternehmen nicht benannt werden. Nach Auskunft des IT-Unternehmens werde die Patientensoftware ebenso von anderen Pflegediensten, u. U. auch in Thüringen, genutzt und sei sehr verbreitet.

Der TLfDI informierte sich bei der Thüringer Herstellerfirma über die Patientensoftware bzw. die zum Einsatz kommende App und bewertete sie technisch und datenschutzrechtlich. Der TLfDI kam zu folgendem Ergebnis:

Der Betrieb und die Betreuung des zentralen Software-Servers erfolgt in der Regel nicht bei der Softwarefirma, sondern beispielsweise direkt beim Pflegedienst bzw. bei größeren Organisationen in einem eigenen Rechenzentrum oder auf einem externen angemieteten Server. In Ausnahmefällen, allerdings nicht im vorliegenden Fall, ist das Softwareunternehmen jedoch bereit, die Wartung der Server zu übernehmen. Daraus ergibt sich für derartige Fälle die datenschutzrechtliche Forderung des TLfDI, einen Vertrag zur Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG) mit dem technischen Betreiber und der Wartungsfirma abzuschließen.

Da es sich bei Patientendaten, die im Rahmen der Pflege anfallen, um besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG handelt, unterliegen diese Daten einem besonderen Schutz. Gemäß § 9 BDSG müssen öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften des BDSG zu gewährleisten. Somit ergibt sich für den TLfDI datenschutzrechtlich die Forderung nach § 9 BDSG an die verantwortlichen Stellen in derartigen Fällen, die Daten in der Datenbank zu verschlüsseln und den Personenkreis mit

dem notwendigen Wissen für den Zugriff so gering wie möglich zu halten. Die zentrale Datenbank ist auf Wunsch des Kunden, der nach geltendem Recht immer die verantwortliche Stelle ist, zu verschlüsseln. Das bedeutet, dass der Kunde ermitteln muss, ob aufgrund des Schutzbedarfs der Daten eine Verschlüsselung erforderlich ist, wovon bei den in Rede stehenden Daten auszugehen ist. Die Datenübertragung vom Web-Portal und der Smartphone-App soll ebenfalls verschlüsselt über HTTPS erfolgen. Datenschutzrechtlich ergab sich hierbei für den TLfDI die Forderung, HTTPS in jedem Fall zu nutzen, in dem der Web-Client nicht im selben internen Netz wie der Server betrieben wird. Der Browser übernimmt in diesem Fall die Prüfung der Authentizität, d. h. ob die Daten von der erwarteten Quelle stammen. Die App muss immer HTTPS nutzen, da sie regelmäßig nicht über das interne Netzwerk kommuniziert. Gerade die HTTPS-Nutzung war jedoch technisch zu diesem Zeitpunkt nicht gegeben. Die Datenübertragung vom Client-PC zum Server erfolgte in der Regel unverschlüsselt über die SQL-Schnittstelle des Servers. Dies ist nach Auffassung des TLfDI datenschutzrechtlich sehr bedenklich, wenn die Client-zu-Server-Verbindung nicht innerhalb des internen Netzwerks des Pflegedienstes zustande kommt. Wird der Server bei einem externen Anbieter betrieben, wäre eine Virtuelle-Private-Netzwerk-Verbindung (VPN) zum externen Anbieter notwendig, um eine sichere Verbindung vom Client zum Server zu gewährleisten.

Zum Zeitpunkt der Bewertung des TLfDI wurden bei der App-Nutzung nur Stammdaten (Wer ist zu pflegen?), Tourdaten (Welche Route wurde gefahren?) und Leistungsdaten (Welche Pflegeleistungen wurden summarisch erbracht?) vom Smartphone an den Server übertragen. Die Authentifizierung der Mitarbeiter ist über PIN/Passwort und Nutzernamen möglich. Nach Auffassung des TLfDI sollte die minimale Passwortlänge grundsätzlich den Forderungen des Bundesamtes für Sicherheit in der IT (BSI) folgen.

Auf den mobilen Endgeräten werden die Daten unverschlüsselt gespeichert. Auf den Client-PCs erfolgt die Löschung der Daten beim „Verlassen der Browsersitzung“, ohne dass dabei klar wird, wann dies geschieht. Im Sinne des Datenschutzes sollte der Löschzeitpunkt präzisiert werden. Eine automatisierte Funktion zur Datenlöschung auf Serverseite gibt es nicht. Daraus ergab sich für den TLfDI die datenschutzrechtliche Forderung, dass die Thüringer Softwarefirma mittel- bis langfristig eine einstellbare Löschfunktion einrichten

sollte. Eine Verschlüsselung auf dem Smartphone befand sich zum Zeitpunkt der Bewertung durch den TLfDI in der Entwicklung. Ob eine Verschlüsselung der gespeicherten Daten auf dem Smartphone zu fordern ist, wurde der datenschutzrechtlichen Bewertung der für den Pflegedienst, bei dem die App zum Einsatz kommt, zuständigen Aufsichtsbehörde in Sachsen-Anhalt überlassen. Für die datenschutzrechtliche Aufsicht über die Softwarefirma ist der TLfDI zuständig.

Patientendaten sind besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG und unterliegen als Gesundheitsdaten einem besonderen Schutz. Gemäß § 9 BDSG müssen öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften des BDSG zu gewährleisten. Hierzu zählen neben den Maßnahmen zur Verschlüsselung auch die Regelung des Datenzugriffs und die technische Umsetzung einer angemessenen Löschfrist. Im vorliegenden Fall sind hier noch Nachbesserungen notwendig.

10.6 Einsicht in die Patientenakte – beim Therapeuten oder bei dessen Anwalt?

Ein Patient wollte bei seinem dem Berufsgeheimnis unterliegenden Therapeuten Einsicht in seine Patientenakte nehmen. Der Therapeut verwies ihn an seinen Anwalt, bei dem sich die Akte befände. Damit war klar, dass der Therapeut die Gesundheitsdaten an seinen Anwalt weitergegeben hatte. Um diese Übergabe seiner sensiblen Gesundheitsdaten vom Therapeuten an dessen Anwalt datenschutzrechtlich prüfen zu lassen, wandte sich der betroffene Patient an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Selbstverständlich steht jedem Patienten das Einsichtsrecht in die Patientenakte gemäß § 630g Bürgerliches Gesetzbuch (BGB – sog. Patientenrechtegesetz) zu. Die gesetzlichen Vorschriften gehen grundsätzlich von einer Einsichtnahme beim jeweiligen Berufsgeheimnisträger aus. Dies vor dem Hintergrund, dass nur der die Akte führende Berufsgeheimnisträger auch beurteilen kann, ob einer Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebli-

che Rechte Dritter entgegenstehen. Daher stellte sich die Frage, weshalb der Beschwerdeführer zwecks Akteneinsicht an den Rechtsanwalt verwiesen wurde.

Patientenunterlagen können sich aus verschiedenen Gründen bei einem von einem Berufsgeheimnisträger beauftragten Rechtsanwalt befinden. Soll eine Rechtsfrage geklärt werden, kann ein Berufsgeheimnisträger selbstverständlich einen Rechtsanwalt damit befassten. Zu diesem Zweck können dem Rechtsanwalt die erforderlichen Angaben aber auch nur diese übergeben werden. Steht eine Rechtsstreitigkeit (beispielsweise ein Arzthaftungsprozess oder die Geltendmachung von Honoraren) im Hintergrund, können ausnahmsweise auch alle Angaben in der Patientenakte für die prozessuale Vertretung erforderlich sein. Nach § 3 Abs. 3 Bundesrechtsanwaltsordnung hat jedermann im Rahmen der gesetzlichen Vorschriften das Recht, sich in Rechtsangelegenheiten aller Art durch einen Rechtsanwalt seiner Wahl beraten und vor Gerichten, Schiedsgerichten oder Behörden vertreten zu lassen. Ohne die erforderlichen Unterlagen könnte das Mandat durch den Rechtsanwalt nicht wahrgenommen werden. Ob und in welchem Umfang einem Patienten Auskunft aus oder Einsicht in seine Patientenakte nach § 630b BGB gewährt werden muss und kann, bedarf allerdings als abstrakte Rechtsfrage grundsätzlich keiner Einsicht in die Patientenakte durch den beratenden Rechtsanwalt. In allen anderen Fällen hängt eine Übergabe von Patientendaten an einen Rechtsanwalt ebenso wie jede Datenübermittlung zwischen Berufsgeheimnisträgern (z. B. Arzt zu Arzt, Psychologe oder Psychotherapeut zu Kollegen etc.) davon ab, ob eine Einwilligung des Patienten vorliegt. Liegt keine Einwilligung vor, wäre eine Strafbarkeit aufgrund der Verletzung von Privatgeheimnissen gemäß § 203 Abs. 1 Nr. 2 Strafgesetzbuch (StGB) möglich, was auf Antrag von den Strafverfolgungsbehörden zu prüfen ist.

Auf das Auskunftersuchen des TLfDI nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) teilte der behandelnde Therapeut mit, die Patientenakten würden in seiner Praxis grundsätzlich in einem verschließbaren Stahlschrank aufbewahrt. Weiterhin wurde jedoch der TLfDI um Verständnis dafür gebeten, dass keine weiteren Angaben zum Umstand der Einsichtsgewährung durch den Rechtsanwalt gemacht würden, da eine sachgerechte Beantwortung mit dem Berufsgeheimnis und damit mit der Schweigepflicht kollidieren würde.

Damit gab sich der TLfDI selbstverständlich nicht zufrieden. Er wies darauf hin, dass die Aufsicht nach § 38 BSGS grundsätzlich unab-

hängig von etwaigen Berufs- und Amtsgeheimnissen bestehe. Damit können auch Geheimnisträger im Sinne des § 203 StGB ebenso uneingeschränkt der Datenschutzaufsicht nach § 38 BDSG wie jede andere nicht-öffentliche Stelle unterliegen. Soweit neben den allgemeinen Regeln des BDSG für diese Personengruppen, z. B. Ärzte und Psychotherapeuten, bereichsspezifische Schweige- und Geheimhaltungsverpflichtungen gelten, werden hierdurch die allgemeinen Regeln des BDSG nur punktuell berührt. Der TLfDI forderte daher nochmals dazu auf, die Beantwortung der gestellten Fragen nachzuholen. Dies wurde unter Verweis auf eine Entscheidung des Kammergericht Berlin aus dem Jahr 2010, nach der ein **Rechtsanwalt** wegen § 38 Abs. 3 Satz 2 BDSG grundsätzlich nicht verpflichtet ist, dem Datenschutzbeauftragten mandatsbezogene, seiner Verschwiegenheitspflicht unterliegende Informationen zu geben, erneut verweigert. Seine Verschwiegenheitsverpflichtung bewertete der behandelnde Therapeut genauso wie diejenige der Rechtsanwälte. Dabei wurde allerdings nicht beachtet, dass der Entscheidung des Kammergerichts Berlin zugrunde lag, dass Rechtsanwälte auch Organe der Rechtspflege sind, was für andere Berufsgeheimnisträger jedoch nicht zutrifft. Zugleich drehte der Therapeut den Spieß um und bat den TLfDI um Beratung und forderte eine Versicherung, dass er sich nicht strafbar mache, wenn er das Auskunftsbegehren beantworte. Der TLfDI konnte die Zwangslage des Therapeuten durchaus verstehen und versuchte, den Interessenkonflikt zu entschärfen, indem er den Beschwerde führenden Patienten bat, dem behandelnden Therapeuten eine Schweigepflichtentbindung gegenüber dem TLfDI zu erteilen. Daraufhin teilte der Patient mit, dass er gegen den Therapeuten im Übrigen Strafanzeige erstattet habe. Da die Staatsanwaltschaft eindeutig festgestellt hatte, dass die Unterlagen vom Therapeuten nicht unbefugt an den Rechtsanwalt gelangt waren und somit auch kein Verstoß gegen datenschutzrechtliche Vorschriften vorlag, war das Verwaltungsverfahren durch den TLfDI einzustellen.

Einsicht in die Patientenakte hat nach § 630g BGB der behandelnde Berufsgeheimnisträger zu gewähren. Nur dieser kann einschätzen, ob eine Beschränkung der Akteneinsicht erforderlich und zulässig ist. Allein zur Gewährung der Akteneinsicht bedarf es keines rechtlichen Beistands.

10.7 Fotoshooting in der Arztpraxis – wenn der Patient ungewillt zum Model wird

Ein Bürger beschwerte sich darüber, dass eine Arztpraxis bei der Anmeldung Fotos von den Patienten fertigen würde. Auf Nachfrage wäre ihm mitgeteilt worden, dass die Fertigung der Fotos für die Patientenkartei nötig wären. Das Foto auf der Versicherungskarte sei dafür nicht geeignet. Insbesondere, so der Patient gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), werde gegenüber den Patienten der Eindruck vermittelt, ohne eine entsprechende Zustimmung zur Fotoaufnahme würde keine ärztliche Behandlung stattfinden bzw. kein Termin zu bekommen sein. Der Bürger bat nun den TLfDI um rechtliche Bewertung.

Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Praxis und bat um Stellungnahme zum Sachverhalt und um Mitteilung der Rechtsgrundlage für die Anfertigung von Fotoaufnahmen.

Daraufhin teilte die Praxis mit, dass sie die Vorwürfe mit Nachdruck zurückweise. Weiterhin teilte sie mit, dass die Mitarbeiterinnen bei der Anmeldung angehalten sind, alle Patienten zu fragen, ob ein Foto für die Patientenakte gefertigt werden darf. Besteht kein Einverständnis des Patienten, wird dies von den Mitarbeiterinnen in der Patientenakte vermerkt. Durch diesen Vermerk wird der Patient auch bei erneuter Vorstellung nicht noch einmal gefragt. Ebenfalls befindet sich – für alle Patienten sichtbar und zur Information – an der Anmeldung ein Schild mit einem entsprechenden Hinweis auf das Foto und die Möglichkeit, dies abzulehnen. Weiterhin wurde mitgeteilt, dass – entgegen der Behauptungen – kein Zwang zur Fotodokumentation bestehe. Das erstellte Foto befinde sich ausschließlich in der jeweiligen Patientenakte und unterliege dem Datenschutz und der ärztlichen Schweigepflicht. Als Begründung für die Erstellung der Fotos nannte man die Erhöhung der Patientensicherheit und das sie dazu dienen sollen, Verwechslungen der Patienten und damit einhergehende Behandlungsfehler zu vermeiden. In der Praxis wurde vermehrt festgestellt, dass die Fotos auf den Versicherungskarten häufig nicht dem Erscheinungsbild des Patienten entsprechen. Patienten, die kein Einverständnis zu einem Foto für die Patientenakte erteilen, würden selbstverständlich in der Praxis behandelt und bekommen auch Termine.

Nachdem der TLfDI die Stellungnahme der Praxis rechtlich bewertet hatte, wurde der Praxis mitgeteilt, dass das bisherige Vorgehen nicht den Anforderungen des BDSG entspricht. Denn die Schriftform ist – zumindest in solchen Fällen – für die Einwilligung verbindlich vorgeschrieben, § 4a Abs. 1 BDSG. Bei der Befragung der Patienten und dem daraufhin erteilten Einverständnis zur Anfertigung eines Fotos handelt es sich aber allenfalls um eine mündliche Einwilligung. Ausnahmen von der vorgeschriebenen Schriftform sieht das BDSG jedoch nur vor, wenn wegen besonderer Umstände eine andere Form angemessen ist. Dies ist bei Geschäften unter Anwesenden jeglicher Art kaum der Fall. Die mündlichen Absprachen hinsichtlich der Fotos mit den Patienten entsprachen folglich zumindest nicht der notwendigen Form und waren damit nichtig, § 125 Bürgerliches Gesetzbuch. Diesem Umstand könnte aber Abhilfe geleistet werden, indem eine schriftliche Einwilligung der Patienten, die auch im Übrigen den Anforderungen des § 4a BDSG entspricht, eingeholt würde. Dann wäre die Anfertigung der Fotos datenschutzrechtlich nicht mehr zu beanstanden.

Die Praxis hat sodann auf Raten des TLfDI ein entsprechendes Formular erarbeitet, das den Patienten vorgelegt wird und, mithilfe dessen er der Fotoaufnahme schriftlich zustimmen kann.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Aufgrund einer wirksam erteilten Einwilligung der Patienten ist daher auch die Aufnahme und Speicherung eines Fotos des Patienten möglich. Allerdings ist eine solche Einwilligung nur wirksam, wenn sie die Anforderungen des § 4a BDSG, insbesondere auch die dortigen Formvorschriften erfüllt. Danach bedarf es für eine wirksame Einwilligung grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, vgl. § 4a Abs. 1 Satz 3 BDSG.

10.8 Fotoshooting in der Arztpraxis

Nicht schlecht staunte ein Patient bei seinem Besuch in einer Arztpraxis, als er beobachtete, wie am Empfangstresen die Patienten der Praxis mit einer Fotoaufnahme überrascht wurden. Auf Nachfrage der Patienten beim Praxispersonal, wozu derartige Fotos benötigt

würden, wurden diese mit der Antwort „Es sei für die Patientenkarrei“ abgefertigt. Damit wandte sich ein Betroffener an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Aufklärung dieses Vorfalles und ggf. um Erläuterung der rechtlichen Hintergründe, siehe TB Beitrag 10.7.

Bei dieser Gelegenheit schilderte er auch ein weiteres „Shooting“, bei dem im Rahmen eines OP-Vorbereitungsgespräches plötzlich und ohne Vorwarnung vom Fragenden mittels eines Tablets ein Foto von ihm geschossen wurde. Auch in dieser Praxis wurde ihm auf Nachfrage lediglich geantwortet, dass die Fotos gebraucht würden. Der TLfDI wandte sich daher an die Arztpraxis und forderte diese dazu auf, unter Darlegung der rechtlichen Grundlagen ihr fotografisches Engagement näher zu erläutern. Daraufhin teilte die Praxis mit, dass sie aufgrund von Richtlinien, berufsständischen Vorgaben der Bundes- und Landesärztekammer sowie der Kassenärztlichen Vereinigung verpflichtet sei, ein Risikomanagementsystem einzurichten und umfassende Qualitätssicherungsmaßnahmen zum Schutz der Patienten und zur Vermeidung von Behandlungsfehlern zu ergreifen. Es sei im Rahmen von Präventionsmaßnahmen notwendig, die Fotos zu erstellen, da die Möglichkeiten der eindeutigen Identifizierung des Patienten in Bezug auf die Therapie grundlegend zur Vermeidung von Fehlern sind. Die Praxis gab weiterhin an, dass im schriftlichen Behandlungsvertrag, welcher aber zumeist erst kurz vor der OP abgeschlossen wird, die Einwilligung der Patienten zur Erstellung von Bildaufnahmen eingeholt würde. Nach Prüfung der von der Praxis angegebenen Richtlinien und berufsständischen Vorgaben konnten daraus allerdings seitens des TLfDI keine rechtlichen Grundlagen für die Erstellung von Patientenfotos ohne ausdrückliche Einwilligung abgeleitet werden. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Da sich keine Rechtsgrundlage zur Erhebung von Patientenfotos im Sinne des § 4 Abs. 1 BDSG aus den von der Praxis vorgetragenen Grundlagen ergibt, ist allein auf eine Einwilligung der Patienten abzustellen. Diese Einwilligung muss den Anforderungen des § 4a BDSG entsprechen und ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, nachdem er über den Zweck der Erhebung und Verarbeitung hingewiesen wurde, und schriftlich erfolgt. Weiterhin muss die Einwilligung vor der Erhebung der Da-

ten, also vor dem Fotoshooting, erfolgen. Der Praxis wurde daher aufgegeben, Patientenfotos nur mit vorheriger schriftlicher Einwilligung der Patienten zu fertigen, da eine nachgeholte Einwilligung im schriftlichen Behandlungsvertrag nicht ausreichend ist.

Es bedarf für die Zulässigkeit der Anfertigung von Patientenfotos immer einer vorherigen, aufgeklärten, freiwilligen und schriftlichen Einwilligung des jeweiligen Patienten.

10.9 Datenspeicherung in Apotheke: Kommerz versus Recht

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Apothekenkunden, welcher dort mit einem Rezept ein Arzneimittel kaufen wollte. Beim Suchen des Apothekers nach dem Medikament im Computer wurde er mit der beiläufigen Mitteilung überrascht, dass er das Medikament ja schon einmal bekommen hätte. Auf die Nachfrage des Kunden, wieso sein Name und die von ihm gekauften Medikamente in der Apotheke gespeichert sind, wurde ihm nur ausweichend geantwortet. Der Kunde widersprach daraufhin der Datenspeicherung noch vor Ort und der Apotheker vermerkte dies auch so.

Der Kunde trat daraufhin an den TLfDI heran mit der Frage, ob es überhaupt zulässig sei, dass die Apotheke speichert, welche Medikamente er dort kauft? Er teilte weiterhin mit, dass er weder eine Kundenkarte habe noch jemals irgendeine Zustimmung abgegeben hätte.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Insbesondere erfolgt die Datenerhebung und -verarbeitung in Arztpraxen, Krankenhäusern und auch Apotheken in einem besonders sensiblen Bereich, denn bei Patientendaten und den darin enthaltenen Informationen zum Gesundheitszustand des Patienten handelt es sich um besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG. Aus der Sensibilität der Daten resultiert ein besonderes Schutzbedürfnis, das sich datenschutzrechtlich in § 28 Abs. 6 ff. BDSG niederschlägt. Dort sind strenge Voraussetzungen festgelegt, nach denen im medizinischen Bereich mit Patientendaten verfahren werden darf. Ein Verstoß gegen die Vertraulichkeit der erhobenen

Informationen ist zudem in § 203 Abs. 1 Nr. 1 Strafgesetzbuch mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht. Unter diese Bestimmungen fällt auch der Apotheker.

Die Erhebung sowie die Verarbeitung, worunter auch das Speichern fällt, von besonderen Arten personenbezogener Daten darf nach § 28 Abs. 7 Satz 1 und 2 BDSG nur erfolgen, wenn sie für medizinische Zwecke erforderlich ist und wenn sie von den in der Vorschrift bezeichneten Stellen der Gesundheitsversorgung durchgeführt wird. Die Erhebung und Speicherung der Patientendaten in der Apotheke ist jedoch nicht für medizinische Zwecke erforderlich.

Im Ergebnis ist eine Speicherung von Kundendaten, die besondere Arten personenbezogener Daten enthalten, durch die Apotheke ohne Einwilligung des Kunden nicht zulässig.

Möchte aber eine Apotheke diese Kundendaten speichern, muss eine schriftliche Einwilligung des Kunden gem. § 4a BDSG eingeholt werden. Die Einwilligungserklärung muss den Namen und die Adresse der Apotheke sowie den Grund für die Speicherung enthalten. Auch muss ein Hinweis auf die Möglichkeit des jederzeitigen Widerrufs der Einwilligungserklärung gegeben werden. Soweit Kundendaten ohne dazugehörige Einwilligungserklärungen angelegt werden, handelt es sich um eine rechtswidrige Datenerhebung bzw. -speicherung. Bei einem Widerruf müssen die Daten unverzüglich gelöscht werden.

Etwas anderes gilt nur dann, wenn die Datenspeicherung zur Abwicklung des Vertragsverhältnisses zwischen Kunde und Apotheke erforderlich ist. Hier regelt § 28 Abs. 1 Nr. 1 BDSG die Speicherung für eigene Geschäftszwecke des Apothekers. Dies ist immer dann gegeben, wenn die Speicherung der Daten zur Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich ist und es sich hierbei um personenbezogene Daten handelt und nicht um Gesundheitsdaten. Dies ist dann der Fall, wenn zum Beispiel eine gesonderte Bestellung der Medikamente erfolgte und die Daten (Adresse, Telefonnummer des Kunden) aufgrund der Abwicklung des bestehenden Vertragsverhältnisses noch benötigt werden und daher auch erforderlich sind.

Vorliegend war jedoch eine Speicherung der Kundendaten weder aufgrund einer Einwilligung möglich, da diese nicht erteilt wurde, noch aufgrund der Abwicklung eines gesonderten Bestellvorganges. Die Datenspeicherung erfolgte daher rechtswidrig. Ein Bußgeldverfahren wurde jedoch nicht eingeleitet, da der Kunde die Apotheke

nicht benannt und nur eine allgemeine Anfrage an den TLfDI formuliert hatte.

Die Speicherung von Kundendaten in der Apotheke ist nur mit einer ausdrücklichen Einwilligung des Betroffenen zulässig, da die Erhebung und Speicherung der Patientendaten in der Apotheke nicht für medizinische Zwecke erforderlich ist. Etwas anderes gilt nur dann, wenn die Datenspeicherung zur Abwicklung des Vertragsverhältnisses zwischen Kunde und Apotheke erforderlich ist, beispielsweise im Rahmen einer Bestellung von Medikamenten.

10.10 Daten im Wartezimmer?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde, dass eine Zahnarztpraxis in Thüringen keine räumliche Trennung zwischen dem Wartebereich und dem Patientenaufnahmebereich vorgenommen hatte.

Grundsätzlich müssen Ärzte bei der Organisation ihrer Praxis den Anforderungen des Geheimnis- und Datenschutzes gerecht werden. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung, unter welche auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei personenbezogenen Daten besonderer Art, zu denen auch Gesundheitsdaten zählen (§ 3 Abs. 9 BDSG), ist in besonderem Maße auf das informationelle Selbstbestimmungsrecht der Patienten zu achten.

Gemäß § 9 BDSG haben nicht-öffentliche Stellen, die selbst personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetz, insbesondere die in der Anlage 1 zu § 9 BDSG genannten Anforderungen, zu gewährleisten. Maßnahmen sind nur erforderlich, solange ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Praktisch bedeutet dies, dass Ärzte dafür Sorge tragen müssen, dass unbefugte Dritte keinen Einblick in oder Zugriff auf Patientenakten und -daten haben dürfen. Infolgedessen muss auch bei der Ausrichtung des PC-Bildschirms beachtet werden, dass niemand außer dem

Arzt und dem Praxispersonal Einsicht darin hat. Des Weiteren dürfen keine Gespräche mit den Patienten geführt werden, die über Terminabsprachen hinausgehen, wenn die Möglichkeit des Mithörens besteht.

Auf Nachfrage erklärte die Ärztin, dass wegen der eingeschränkten Platzverhältnisse keine vollständige Trennung des Aufnahme- und Wartebereichs umsetzbar sei. Da es sich um Mieträume handele, wäre eine bauliche Veränderung im Auftrag der Ärztin nicht möglich. Es wurde versichert, dass an der Rezeption lediglich organisatorische Themen besprochen und alle medizinisch relevanten Informationen im Behandlungszimmer ausgetauscht werden.

Somit hat die Ärztin in diesem Fall alle erforderlichen Maßnahmen getroffen. Eine Auseinandersetzung mit dem Vermieter über eine kostenintensive Umbaumaßnahme zu verlangen, wäre im Sinne von § 9 BDSG ein unverhältnismäßiger Aufwand für die verantwortliche Stelle.

Wenn Daten erhoben, verarbeitet oder genutzt werden, müssen auch in einer Arztpraxis technische und organisatorische Maßnahmen getroffen werden, die erforderlich sind, um die personenbezogenen Daten zu schützen (§ 9 BDSG). Eine abschließende Auflistung der entsprechenden Maßnahmen findet sich in der Anlage 1 zu § 9 des BDSG.

10.11 Datenschutz beim Zahnarzt: TLfDI bohrt nach

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt das Schreiben einer Bürgerin, die sich darüber beklagte, dass in einer Arztpraxis der Wartebereich nicht baulich vom Aufnahme-/ Empfangsbereich getrennt sei. Es sei wohl dadurch möglich, dass andere Patienten die Gespräche zwischen Zahnarthelferinnen und Patienten bei der Anmeldung mithören könnten. Der TLfDI wandte sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Praxis. Danach sind die Aufsichtsbehörden – wie der TLfDI – befugt, bei den der Kontrolle unterliegenden Stellen Auskunft zu verlangen. Der TLfDI teilte der Praxis im Auskunftsverlangen mit, dass die wesentlichen rechtlichen Grundlagen für den Umgang mit personenbezogenen Daten in Arztpraxen sich im BDSG wiederfinden. Das BDSG regelt, wie mit personenbezogenen Daten durch die

verantwortlichen Stellen und ggf. ihre Mitarbeiter umzugehen ist. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung, worunter auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene nach § 4a BDSG eingewilligt hat.

Dabei hat auch die Praxisorganisation den Anforderungen des Geheimnis- und Datenschutzes gerecht zu werden. Denn gerade bei Gesundheitsdaten als besondere Art personenbezogener Daten, § 3 Abs. 9 BDSG, wollen die Patienten den Umgang mit ihren sensiblen Daten geschützt wissen. Dem Datenschutz muss der Arzt dadurch Rechnung tragen, dass er sowohl bei konventionellen Patientenakten als auch beim Einsatz von Datenverarbeitungstechniken gewährleistet, dass unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Kenntnis von den Patientendaten erhalten. Unbefugte Dritte sind dabei auch andere Patienten. So dürfen papiergebundene Patientenakten in keinem Fall so gelagert werden, dass andere Patienten diese zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. In den Fällen, in denen ein Arbeitsplatz nicht besetzt ist, muss der EDV-Arbeitsplatz gesperrt und Akten müssen weggeschlossen werden, sodass wartende Patienten keine Möglichkeit haben, Patientendaten zur Kenntnis zu nehmen. Ebenso können, wenn der Wartebereich und der Anmeldebereich nicht getrennt sind, keine Gespräche mit dem Patienten geführt werden, die über reine organisatorische Themen, wie beispielsweise Terminabsprachen, hinausgehen. Weiterhin wurde der Praxis mitgeteilt, dass bei der Organisation der Praxis sicherzustellen ist, dass unbefugtes Mitlesen oder Mithören ausgeschlossen wird.

Die Praxis reagierte mit Verwunderung über das Schreiben des TLF-DI und teilte mit, dass an der Rezeption in der Regel keine weiterführenden Gespräche über Patienten geführt werden würden. Der Computerbildschirm sei für die Patienten nicht einsehbar und in der Rezeption integriert. Die für die Sprechstunde vorbereiteten Patientenakten würden nicht einsehbar für die an der Rezeption stehenden Patienten im hinteren Bereich der Karteikartenschränke liegen. Der Wartebereich war durch ein Möbelstück abgetrennt, allerdings wurde aus Platzgründen diese Trennung wieder rückgängig gemacht. Ebenso konnten dadurch allein wartende Kinder vom Personal besser beaufsichtigt werden. Die Rezeption sei in der Regel während der

Sprechstunde immer besetzt. Nicht ausgeschlossen sei aber das kurzzeitige Verlassen der Rezeption durch die Schwester, um Patientenakten in das Sprechzimmer zu bringen. Die Rezeption für diesen kurzen Zeitraum abzuschließen, sei bei dem Patientendurchlauf schlicht und ergreifend nicht möglich. Der Arzt versicherte, seine Mitarbeiter über den Inhalt des Schreibens zu informieren und sie auch diesbezüglich aktenkundig zu belehren. Die bauliche Veränderung bezüglich der Abtrennung wird er umgehend rückgängig machen.

Der TLfDI behält sich eine Vor-Ort-Kontrolle vor.

In Arztpraxen werden regelmäßig Patientendaten verarbeitet. Diese Daten stehen als besondere Art von personenbezogenen Daten – § 3 Abs. 9 BDSG – unter dem besonderen Schutz des BDSG. Deshalb ist auch hier gemäß § 4 Abs. 1 BDSG die Erhebung, Verarbeitung, worunter auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene nach § 4a BDSG eingewilligt hat.

10.12 Auch Krankenhäuser von DS-GVO betroffen

Die Landeskrankenhausesgesellschaft erreichte eine Nachfrage eines Thüringer Krankenhauses im Hinblick auf die neue EU-Datenschutz-Grundverordnung (DS-GVO). Die Krankenhausesgesellschaft leitete die Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter.

Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie doch erhebliche Unterschiede bestanden, soll mit der DS-GVO das Datenschutzrecht in der EU vereinheitlicht werden. Sie wird ab 25. Mai 2018 wirksam.

In Art. 35 DS-GVO ist die Datenschutz-Folgenabschätzung, die der Verantwortliche für die Datenverarbeitung beratend mit dem Datenschutzbeauftragten, durchzuführen hat, geregelt. Konkret fragte nun das Krankenhaus, ob die nach Art. 35 Abs. 4 DS-GVO von der Aufsichtsbehörde zu erstellende Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, bereits erstellt ist und falls ja, wo diese zu finden sei.

Der TLfDI erklärte, dass die Liste, in der die Verarbeitungsvorgänge für die Datenschutz-Folgenabschätzung enthalten sind, zu gegebener

Zeit auf der Homepage des TLfDI zu finden sein wird. Noch stimmen sich die Aufsichtsbehörden des Bundes und der Länder darüber ab, welche Verarbeitungsvorgänge einer Datenschutz-Folgenabschätzung zu unterziehen sind, da eine möglichst bundeseinheitliche Handhabung gewünscht ist. Der TLfDI ging aber davon aus, dass die Datenverarbeitung in einem Krankenhaus mit einem Krankenhausinformationssystem einer Datenschutz-Folgenabschätzung zu unterziehen ist. Wenn die Abstimmung unter den Datenschutzaufsichtsbehörden und die Veröffentlichung auf der Homepage des TLfDI erfolgt sind, wird der TLfDI die Krankenhausesellschaft informieren.

Zudem wollte das Krankenhaus wissen, ob durch die neue EU-DS-GVO Handlungsbedarf bei den vorliegenden Standardvertragsklauseln besteht. Die Standardvertragsklauseln der Europäischen Union finden derzeit Anwendung, wenn personenbezogene Daten außerhalb der Europäischen Union verarbeitet werden. Die Klauseln sollen den Schutz persönlicher Daten auch dann sicherstellen, wenn Unternehmen personenbezogene Daten an andere Unternehmen außerhalb der EU zur Weiterverarbeitung übersenden. Im Gegensatz dazu ist der Privacy Shield (Datenschutzschild) ein informelles Übereinkommen der Europäischen Union mit den Vereinigten Staaten von Amerika, in dem die amerikanische Bundesregierung datenschutzrechtliche Zusicherungen abgegeben hat. Amerikanische Unternehmen können sich dazu verpflichten, die Regelungen des Privacy Shield einzuhalten und sich in eine entsprechende Liste eintragen lassen, die unter <https://www.privacyshield.gov/list> veröffentlicht wird. Die Europäische Kommission hat am 12. Juli 2016 beschlossen, dass die Vorgaben des Datenschutzschilds dem Datenschutzniveau der Europäischen Union entsprechen. Außerdem fragte das Krankenhaus, ob getätigte Verträge einschließlich der Auftragsdatenverarbeitung gesichtet und überarbeitet werden müssen. Nach dem Kenntnisstand des TLfDI besteht auch für die vorliegenden Standardvertragsklauseln Anpassungsbedarf hinsichtlich der DS-GVO. Die bisher geschlossenen Verträge müssten daher gesichtet und überarbeitet werden. Dies gilt dann auch insbesondere für die Auftragsverarbeitung. Hierzu soll in Zusammenarbeit mit den anderen Aufsichtsbehörden eine Handlungsempfehlung erarbeitet werden.



Mit Inkrafttreten der DS-GVO müssen viele Regelungen hinsichtlich des Datenschutzes angepasst werden. Die Liste der Verarbeitungsvorgänge, in denen die Datenschutz-Folgenabschätzung durchgeführt werden muss, wird auf der Homepage des TLfDI zu finden sein. Da die DS-GVO viele Änderungen enthält, müssen auch die bereits geschlossenen Verträge und Standardklauseln hinsichtlich der neuen datenschutzrechtlichen Regelungen geprüft und gegebenenfalls geändert werden.

10.13 Schreddern im Krankenhaus

Die Datenschutzbeauftragte eines thüringischen Klinikums bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft zur Frage der ordnungsgemäßen Vernichtung von Datenträgern. Sie hatte sich bereits selbst über die geltenden Regelungen im Internet informiert und dabei die „Orientierungshilfe zur Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung“ (OH) gefunden. In der OH werden Anforderungen an die datenschutzgerechte Vernichtung von Datenträgern dargelegt, die berücksichtigen, dass im Oktober 2012 die neue DIN 66399 „Büro- und Datentechnik – Vernichten von Datenträgern“ veröffentlicht wurde. Die DIN 66399 empfiehlt jeder verantwortlichen Datenverarbeitenden Stelle, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs zu klassifizieren; sie definiert hierfür drei Schutzklassen. Darüber hinaus beschreiben sieben Sicherheitsstufen Anforderungen an die Wirksamkeit der Vernichtung, d. h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Information zur Kenntnis nehmen zu können. Anschließend empfiehlt die DIN, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten und trägt so dem Prinzip der Angemessenheit Rechnung. Die DIN bestimmt für diverse Materialklassen (wie Papier, Mikrofilm, magnetische Datenträger, optische Datenträger, Halbleiterspeicher) Grenzwerte für Teilchengrößen, die bei der Vernichtung eines Datenträgers eingehalten werden müssen, um die Wiederherstellung von Informationen aus dem nach der Vernichtung vorliegenden Restmaterial zu verhindern oder zumindest zu erschweren.

Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, kommen verantwortliche Stellen nach § 20 Abs. 2 Bundesdatenschutzgesetz (BDSG) ihrer Verpflichtung zum Löschen dieser Daten nach. Personenbezogene Daten sind insbesondere dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Unter dem Begriff „Löschen“ wird dabei die Unkenntlichmachung gespeicherter personenbezogener Daten verstanden (§ 3 Abs. 4 Nr. 5 BDSG). Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit nach § 9 BDSG sowie dessen Anlage). Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten.

Die Datenschutzbeauftragte wollte wissen, welche Anforderungen danach für das betreffende Krankenhaus gelten. Nach Auffassung des TLfDI sind alle personenbezogenen medizinischen Daten, die einem Berufs- und/oder Amtsgeheimnis unterliegen, der Schutzbedarfsklasse 2 bis 3 zuzuordnen. Dies sind z. B. Behandlungsunterlagen und- Diagnosen. Spezielle Unterlagen, die z. B. Transplantationen betreffen, sind Schutzbedarfsklasse 3 zuzuordnen. Andererseits gibt es Gesundheitsdaten, die nicht dem Berufs- und/oder Amtsgeheimnis unterliegen, wie z. B. Blutspendeaufzeichnungen, die entsprechend der OH nach Schutzbedarfsklasse 2 einzuordnen sind. Es kommt also auf den Einzelfall an.

Zur Erfüllung der Schutzbedarfsklasse 2 wird die Sicherheitsstufe ab P-4 aufwärts empfohlen. Zur Erfüllung der Schutzbedarfsklasse 3 ist aus Sicht des TLfDI die Sicherheitsstufe ab P-5 aufwärts einzusetzen. Entsprechend der DIN 66399-2 bedeutet dies konkret:

Sicherheitsstufe für Papier	Materialteilchenfläche	Toleranz für 10% des Materials
P-4	Die Materialteilchenfläche $\leq 160 \text{ mm}^2$ und für die regelmäßigen Partikel: Streifenbreite max. 6mm	Materialteilchenfläche max. 480 mm^2

P-5	Die Materialteilchenfläche $\leq 30 \text{ mm}^2$ und für die regelmäßigen Partikel: Streifenbreite max. 2mm	Materialteil- chenfläche max. 90 mm^2
-----	--	---

Der Datenschutzbeauftragten wurden die durch das Krankenhaus einzuhaltenden Anforderungen (Sicherheitsstufe P-5) mitgeteilt.

Auch bei der Datenträgervernichtung sind die datenschutzrechtlichen Vorgaben einzuhalten. Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, kommen verantwortliche Stellen ihrer Verpflichtung zum Löschen dieser Daten nach. Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit), § 9 BDSG sowie dessen Anlage. Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Krankenhäuser müssen in Bezug auf die Gesundheitsdaten die Schutzklasse 3 nach DIN 66399 einhalten.

10.14 Einwilligungserklärung bei Ärzten – So einfach geht das nicht!

Ein externer Datenschutzbeauftragter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um eine Zweitmeinung für einen an ihn herangetragenen Fall zu erhalten. Einer seiner Kunden ist Arzt und bietet individuelle Gesundheitsleistungen und Untersuchungen an. Hierzu muss der Patient einwilligen, dass die Praxis für die Auswertung Informationen von vorherigen Untersuchungen anfordern und zur Auswertung die Daten an einen spezifischen Dritten weitergeben und zurückerhalten darf. Dabei wird der Patient darüber informiert, wer nach seinen Daten angefragt wird und wo die Daten verarbeitet werden.

Die Praxis will die Einwilligung jetzt allerdings dahingehend ändern, dass der Patient nur noch eine pauschale Einwilligung unterschreibt. Somit könnte die Praxis auch nach Abschluss der ersten Untersuchung weiterhin ohne erneute Rückfrage und Einwilligung des Patienten bei den mitbehandelnden Ärzten Daten, Befunde usw. abrufen. Durch die neue Einwilligung könnten alle mit dem Behandlungsfall

verknüpften Daten ohne weitere Zustimmung des Patienten gegebenenfalls lange nach dessen Zustimmung abgefragt werden. Der externe Datenschutzbeauftragte hat dabei Bedenken, da medizinische Daten besonders schützenswert sind.

Der TLfDI informierte darüber, dass der Patient gemäß § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Einwilligung hingewiesen werden muss („informierte Einwilligung“). Sowohl die Verwendungsziele als auch und vor allem die Verarbeitungsfolgen lassen sich erst abschätzen, wenn die jeweils gewünschten Daten genauso wie die Verarbeitungsbedingungen und die potenziellen Übermittlungsempfänger angegeben werden. In der vorgesehenen neuen Einwilligung waren diese Angaben nicht erkennbar. Die Einwilligung erfüllte daher nicht die Voraussetzungen des § 4a BDSG. Sie wäre unwirksam.

Zudem müssten die Ärzte, die Patientendaten an die Praxis übermitteln, ebenfalls eine datenschutzrechtliche Einwilligung und eine Schweigepflichtentbindung bei den betroffenen Patienten einholen bzw. der Patient müsste diese Ärzte von ihrer Schweigepflicht entbinden. Dies kann in einer gemeinsamen Erklärung geschehen, in der der Patient eine bestimmte Stelle ermächtigt, zu einem bestimmten Zweck bei einem bestimmten Arzt Informationen einzuholen, und gleichzeitig in die entsprechende Übermittlung einwilligt.

Die Einschätzung des externen Datenschutzbeauftragten war damit völlig richtig gewesen.

Eine Datenübermittlung von Patientendaten durch eine Arztpraxis an einen Dritten ist mit schriftlicher Einwilligung des Patienten möglich. Nach § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Patient muss darin auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden. Damit der Patient erkennt, wozu seine Daten verwendet werden und wer diese erhält, müssen die konkreten Verarbeitungsbedingungen und die potenziellen Übermittlungsempfänger angegeben werden.

10.15 Erwachsene familienversicherte Patienten sind mündig – eine Erhebung von Hauptversichertendaten entfällt damit!

Eine Bürgerin beschwerte sich darüber, dass eine Zahnarztpraxis ihr anlässlich eines Untersuchungstermins nicht nur ihre eigene, sondern aufgrund der Familienversicherung auch die Krankenversicherten-Karte ihres Ehemanns abverlangte. Die Praxismitarbeiter begründeten dies ihr gegenüber damit, dass das PC-Programm die Daten des Ehemanns für die Rechnungsstellung zwingend benötige.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat die Zahnarztpraxis um eine Stellungnahme zum vorgetragenen Sachverhalt und um Darlegung der Rechtsgrundlage für die Abfrage der personenbezogenen Daten des Ehemannes. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.

Daraufhin informierte die Zahnarztpraxis den TLfDI darüber, dass die Praxis 2016 übernommen worden sei. Im Rahmen der Übernahme sei die Abfrage der familienversicherten Patienten nach dem Hauptversicherten standardisiert mit durchgeführt worden. Auch ein neu eingeführtes Computerprogramm verlangte die Eingabe der Daten des Hauptversicherten, sowohl bei minderjährigen als auch bei erwachsenen Patienten. Den Ärzten sei nicht bewusst gewesen, dass auf die Angabe des Hauptversicherten bei erwachsenen Patienten verzichtet werden kann. Sie waren davon ausgegangen, dass diese Information für die Abrechnung auch bei erwachsenen Patienten notwendig ist.

Im Dezember 2016 installierte die Zahnarztpraxis nach eigener Aussage ein neues Update des Abrechnungsprogramms und entfernte in diesem Zusammenhang die Abfrage nach den Daten des oder der Hauptversicherten bei erwachsenen Patienten.

Der TLfDI teilte der Beschwerdeführerin daraufhin mit, dass die Abfrage nach den Daten der bzw. des Hauptversicherten in der Zahnarztpraxis nun nicht mehr erfolgt, da ein neues Abrechnungsprogramm installiert wurde und dass sich die Mitarbeiter der Praxis für entsprechende Unannehmlichkeiten bei der Beschwerdeführerin entschuldigten. Die Zahnarztpraxis informierte der TLfDI darüber, dass er die Angelegenheit als erledigt ansehe, da die Abfrage der Hauptversichertendaten bei erwachsenen Patienten nun nicht mehr stattfinde.

Die in diesem Falle aufgeworfene Problemstellung zur Abfrage nach Daten der Hauptversicherten bei erwachsenen Patienten sollte nach Auffassung des TLfDI auch mit den Krankenversicherungen diskutiert werden. Daher entschied sich der TLfDI, diese Fragestellung in den Arbeitskreis „Gesundheit und Soziales“ der Datenschutzkonferenz des Bundes und der Länder einzubringen, da die meisten Krankenkassen nicht in die Zuständigkeit des TLfDI fallen.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Im Falle der Familienversicherung von Patienten ist die Abfrage von Daten der oder des Hauptversicherten durch den Arzt im Behandlungsfall bei erwachsenen Patienten datenschutzrechtlich nicht zulässig, weil sich eine entsprechende Ermächtigungsgrundlage weder im BDSG noch im Sozialgesetzbuch findet.

10.16 Beratung durch den Amtsarzt verstößt nicht gegen den Datenschutz

Ein Vater beschwerte sich über eine Amtsärztin und trug gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vor, die Amtsärztin habe in Bezug auf ihn und in Bezug auf seine Tochter persönliche Daten weitergegeben und damit gegen den Datenschutz sowie gegen die ärztliche Schweigepflicht verstoßen. Der Beschwerdeführer gab an, dass er von der Kindesmutter getrennt lebe und beide Elternteile ein gemeinsames Sorgerecht hätten. Die Kindesmutter habe dem Beschwerdeführer anwaltlich mitteilen lassen, dass sie die Übertragung der elterlichen Sorge begehre. Dem entsprechenden anwaltlichen Schreiben habe nach Information des Beschwerdeführers eine Stellungnahme der Amtsärztin beigelegt, aus der hervorging, dass sie betreffend die Tochter des Beschwerdeführers mit zwei weiteren Kinder- und Jugendärzten kommuniziert habe. Dies stellte nach Ansicht des Beschwerdeführers eine Verletzung des Datenschutzes hinsichtlich der persönlichen Daten seiner Tochter und seiner eigenen als sorgeberechtigtem Elternteil sowie eine Verletzung der ärztlichen Schweigepflicht dar. Der Beschwerdeführer gab an, dass er keine persönliche Einwilligung zur Weitergabe seiner Daten erteilt und die Ärztin auch nicht von ihrer Schweigepflicht entbunden hatte.

Der TLfDI bat die entsprechende Stadtverwaltung um Stellungnahme zum vorgetragenen Vorwurf der Datenschutzverletzung durch die Amtsärztin. Die Stadtverwaltung ergänzte und präzierte den vom Beschwerdeführer vorgetragenen Sachverhalt. Im Rahmen der Besuchsregelungen zum geteilten Sorgerecht war zwischen dem Beschwerdeführer und der Kindesmutter ein Vergleich geschlossen worden. Gegenstand des Vergleichs war u. a. die Festlegung, dass die Mutter regelmäßig ein amtsärztliches Attest vorlegen musste, wenn ihre Tochter zu Besuchsterminen beim Beschwerdeführer und Vater des Kindes wegen einer Erkrankung nicht reisefähig war. Daher stellte die Kindesmutter die gemeinsame Tochter regelmäßig bei der Amtsärztin vor gemäß § 3 Gesundheitsdienstverordnung (GesDV), wenn sie aufgrund der Vergleichsregelung ein Attest benötigte. Im Rahmen dieser Untersuchung informierte die Kindsmutter die Amtsärztin auch über die zwei weiteren Fachärzte, die ihre Tochter behandelten, über den Grund der ärztlichen Vorstellung sowie über den Namen und die Adresse des Kindesvaters als ebenfalls sorgeberechtigtes Elternteil. In der Folge dieser Information nahmen die drei Ärztinnen im Hinblick auf die Behandlung des Kindes miteinander Kontakt auf. Die damit verbundene Datenübermittlung zwischen den Ärztinnen an die Amtsärztin war zur ordnungsgemäßen Begutachtung des Kindes und seiner Weiterbehandlung notwendig und nach § 28 Abs. 7 Satz 2 Bundesdatenschutzgesetz zulässig.

Der TLfDI teilte dem Beschwerdeführer mit, dass die Amtsärztin ihre Informationen gemäß § 3 GesDV erlangte und diese Informationen vorschriftsmäßig gemäß § 20 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) im Rahmen der Ausübung ihrer fachlichen Aufgabe als Amtsärztin verwendet hat. Neben der Untersuchung des Kindes und der Erstellung der gerichtlich angeordneten ärztlichen Atteste gemäß § 3 GesDV gehört zur amtsärztlichen Aufgabe auch die gesundheitliche Beratung und Aufklärung von Kindern und deren Sorgeberechtigten im Hinblick auf ihre gesundheitliche Entwicklung gemäß § 8 GesDV. Somit konnte der TLfDI keinen Verstoß gegen den Datenschutz durch die Amtsärztin feststellen.

Gemäß § 20 Abs. 1 ThürDSG ist das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die

Daten erhoben worden sind. Gemäß § 8 GesDV gehört zur amtsärztlichen Aufgabe auch die gesundheitliche Beratung und Aufklärung von Kindern und deren Sorgeberechtigten im Hinblick auf ihre gesundheitliche Entwicklung.

10.17 Ist die Weitergabe der Personaldaten an die Heimaufsicht erlaubt?

Die Leitung eines Seniorenheimes wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da sie mit der für sie zuständigen Heimaufsicht uneinig darüber war, ob die Weitergabe von Personallisten datenschutzrechtlich zulässig ist. Nach § 10 Abs. 3 Thüringer Gesetz über betreute Wohnformen und Teilhabe (ThürWTG) sind den zuständigen Behörden, in dem Fall der Heimaufsicht, vor Eröffnung einer Einrichtung die Namen, die berufliche Ausbildung der Pflege- und Betreuungskräfte mit Geburtsjahr, die vorgesehene Tätigkeit und wöchentliche Arbeitszeit sowie quartalsweise Änderungen personenbezogener Daten aller Mitarbeiter zu melden. Um diese Angaben zu erhalten, sendet die Heimaufsicht den Heimleitern eine vorgegebene Excel-Liste zu, die diese auszufüllen haben. Damit bestehe die Verpflichtung, jährlich eine Personalliste mit vollem Namen, Geburtsdatum, Ausbildung, Einstand, Tätigkeit und Arbeitsstunden der Mitarbeiter zu melden. Quartalsweise müssen Personaländerungen mit denselben Angaben gemacht werden. Jedoch sei unklar, wie lange die personalisierten Daten gespeichert werden, wer sie einsieht, wie sie verarbeitet werden und wann sie gelöscht werden. Die Heimleitung hatte datenschutzrechtliche Bedenken. Sie sei grundsätzlich bereit, der Heimaufsicht die Personalstärke mitzuteilen, allerdings würde sie sich wohler fühlen, die Daten anonymisiert zu versenden, um nicht gegen datenschutzrechtliche Bestimmungen zu verstoßen.

Der TLfDI teilte der Heimleitung mit, dass im Datenschutzrecht gemäß § 4 Abs. 1 BDSG, ein „Verbot mit Erlaubnisvorbehalt“ gelte. Das bedeutet, dass jede Erhebung und Verarbeitung von Daten grundsätzlich unzulässig ist, es sei denn ein Gesetz erlaubt sie bzw. der Betroffene hat eingewilligt.

Das am 24. Juni 2014 in Kraft getretene ThürWTG regelt in § 10 eine Anzeigepflicht von stationären Einrichtungen nach § 2 ThürWTG. Stationäre Einrichtungen im Sinne dieses Gesetzes sind Einrichtungen, die dem Zweck dienen, ältere, pflegebedürftige oder

behinderte oder von Behinderung bedrohte volljährige Menschen aufzunehmen, ihnen Wohnraum zu überlassen sowie mit der Wohnraumüberlassung verpflichtend Pflege- oder Betreuungsleistungen zur Verfügung zu stellen oder vorzuhalten, die in ihrem Bestand von Wechsel sowie Zahl der Bewohner abhängig sind und entgeltlich betrieben werden. Das Gesetz verpflichtet diese Einrichtungen, drei Monate vor der vorgesehenen Inbetriebnahme unter anderem die Namen, die berufliche Ausbildung der Pflege- und Betreuungskräfte mit Geburtsjahr, die vorgesehene Tätigkeit und wöchentliche Arbeitszeit anzuzeigen. Nach Absatz 3 der Vorschrift sind der zuständigen Behörde während des Betriebs quartalsweise Änderungen dieser Angaben anzuzeigen. Eine Begründung für diese gesetzliche Regelung ist in der entsprechenden Landtagsdrucksache (5/7006) zu finden, in der ausgeführt wird, dass die Anzeigepflicht schon nach bisherigem Recht die Aufgabe hatte, die zuständige Behörde über die Aufnahme, Änderung oder Einstellung des Einrichtungsbetriebes zu unterrichten. Dazu benötigt die zuständige Behörde Informationen darüber, ob und wie jemand eine stationäre Einrichtung betreiben will. Der Träger hat sicherzustellen, dass Beschäftigte, vor allem Pflege- und Betreuungskräfte, in ausreichender Zahl vorhanden sind und dass ihre persönliche und fachliche Eignung für die von ihnen zu leistende Tätigkeit ausreicht. Die von der Heimaufsicht geforderten Angaben entsprechen nach Prüfung durch den TLfDI der gesetzlichen Verpflichtung des § 10 ThürWTG und sind damit zulässig. Dies wurde der Heimleitung mitgeteilt.

Im Datenschutzrecht gilt ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Erhebung und Verarbeitung von Daten grundsätzlich unzulässig ist, es sei denn ein Gesetz erlaubt sie bzw. der Betroffene hat eingewilligt. § 10 ThürWTG verpflichtet stationäre Einrichtungen, drei Monate vor der vorgesehenen Inbetriebnahme bestimmte personenbezogene Daten der Pflege- und Betreuungskräfte anzuzeigen.

10.18 Datenverarbeitung im Auftrag – ein Klinikum war gut vorbereitet

Ein Klinikum wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Bewertung hinsichtlich einer Aktenvernich-

tung. Demnach sollten Patientenakten, Verwaltungsakten, Datenträger und Festplatten vernichtet werden. Die Daten hatten die gesetzliche Aufbewahrungsfrist erreicht. Ebenso übersandte das Klinikum dem TLfDI die Angebote und Zertifikate des Vernichtungsunternehmens, woraus ersichtlich wurde, nach welchen Parametern die Vernichtung erfolgen sollte.

Eine Aktenvernichtung stellt nach § 3 Abs. 4 Nr. 5 Bundesdatenschutzgesetz (BDSG) eine Löschung – das Unkenntlichmachen – von gespeicherten personenbezogenen Daten dar. Nach Informationen des Klinikums erfolgt die Löschung der Daten aber nicht durch das Klinikum selbst, sondern durch eine vom Klinikum beauftragte Firma. In solch einem Fall spricht man von einer Datenverarbeitung im Auftrag nach § 11 BDSG. Dieser besagt, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen, die Berichtigung, Löschung und Sperrung von Daten, die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen, die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen, die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags festzulegen sind. Der Vertrag zur Auftragsdatenverarbeitung wurde dem TLfDI zur Kenntnis gegeben und nach Prüfung für gesetzeskonform befunden. Ebenfalls teilte das Klinikum mit, dass der Datenschutzbeauftragte den gesamten Vernichtungsprozess begleiten würde, um

unrechtmäßige Kenntnisnahmen der sensiblen Daten bis zur letzten Vernichtung zu verhindern.

Das generelle Löschen von personenbezogenen Daten ist im § 35 BDSG geregelt. Absatz 2 Nummer 3 besagt, dass jene Daten zu löschen sind, welche für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Hierzu zählt wie in diesem Fall die abgelaufene Aufbewahrungsfrist. Ein besonderes Augenmerk liegt hierbei auf der Art der Daten. Da es sich um Gesundheitsdaten handelt, sind diese Daten nach § 3 Abs. 4 Nummer 9 BDSG als besondere Art der Daten einzustufen und es gilt die DIN 66399 als besondere Regelung für diese Vernichtung. Hierbei sind die zu vernichteten Daten in unterschiedliche Schutzklassen und Sicherheitsstufen einzuordnen. Bei Patientenakten gilt demnach die Schutzklasse 3 und Sicherheitsstufe P5. Das Unternehmen, welches die Akten vernichten sollte, belegte diese Parameter bis ins Detail.

Der TLfDI prüfte das gesamte Vorhaben des Klinikums anhand der Fakten und befand es für datenschutzkonform.

Auch eine Aktenvernichtung stellt nach § 3 Abs. 4 Nr. 5 Bundesdatenschutzgesetz (BDSG) einen datenschutzrelevanten Vorgang dar, nämlich eine Löschung, also das Unkenntlichmachen von gespeicherten personenbezogenen Daten. Auch hier ist auf die datenschutzgerechte Vernichtung und insbesondere auf die unterschiedlichen Schutzklassen und Sicherheitsstufen zu achten, vor allem, wenn es sich wie hier um besondere Arten von personenbezogenen Daten handelt. Eine Datenverarbeitung im Auftrag nach § 11 BDSG liegt vor, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Der Auftraggeber ist für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen beachtet werden muss.

10.19 Bestellung von Arzneimitteln mit WhatsApp

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Apothekenkunden zur datenschutzrechtlichen Zulässigkeit einer Serviceleistung, die in einer Nordthüringer Apotheke angeboten wurde: Arzneimittelvorbestellung mittels WhatsApp. Diese spezielle Dienstleistung wird in den Apothekengeschäften immer beliebter und viele Apotheken bieten ihren Kunden diesen Service an. Sie verkennen dabei jedoch zumeist die datenschutzrechtliche Brisanz dieser Unternehmung. Um mittels WhatsApp die Bestellung aufzugeben, werden die Kunden zumeist dazu aufgefordert, ein Foto vom Rezept oder der Verpackung des bereits vorliegenden Medikamentes zu übersenden. Gleichzeitig werden die Telefonnummer und ggf. auch der Name des Bestellenden übermittelt. Vor allem bei Rezepten handelt es sich um besonders schützenswerte, personenbezogene Daten nach § 3 Abs. 9 BDSG, da Informationen zu den vorliegenden Krankheiten oder dem Gesundheitszustand des Bestellers abgeleitet werden können. Weiterhin wird auch die Telefonnummer als personenbezogenes Datum an WhatsApp und an den Apothekenbetreiber übermittelt. Zusätzlich dazu wird bei der Nutzung von WhatsApp automatisch das lokal hinterlegte Adressbuch des Nutzers mit ausgelesen und alle diese Kontaktdaten ungefragt an WhatsApp übertragen und auf den Servern in Kalifornien/USA gespeichert. Was schlussendlich mit diesen Daten passiert, weiß kein Mensch. Denn trotz der mittlerweile plattformunabhängigen Ende-zu-Ende-Verschlüsselung von Text und Bilddaten erhält WhatsApp Kenntnis von den Metadaten (IP-Adresse, Geräte-ID, Zeitpunkt usw.) Auch aus diesen Daten können Nutzerprofile erstellt werden, Kaufverhalten analysiert und weitere Rückschlüsse auf die Chatbeteiligten gezogen werden. Schlussendlich bleiben vor Ort in der Apotheke noch wichtige Fragen zu klären: Wie ist das Empfangsgerät des Apothekers geschützt? Wer hat Zugriff auf die übermittelten Rezept-Daten? Werden die übermittelten Fotos nach dem Empfang und der Auswertung wieder gelöscht? Die Handhabung der von den Kunden empfangenen, besonders schützenswerten Daten, obliegt den Apotheken. Diese müssen technisch-organisatorische Maßnahmen zur Datensicherheit treffen und umsetzen. Trotz allem ist die Bestellung per WhatsApp ein datenschutzrechtliches Wagnis, da aufgrund der Übertragung der

Daten in die USA deren weitere Nutzung völlig unklar ist und auch ob die Verschlüsselung an sich von Dauer ist.

Aufgrund der Bequemlichkeit des Bestellvorgangs über WhatsApp sind viele Apotheken daran interessiert gewesen, ihren Kunden diese Bestellmöglichkeit anbieten zu können. Die datenschutzrechtlichen Bedenken, die sich aufgrund der Übermittlung an WhatsApp ergeben, wurden seitens der Apotheker oft übersehen. Daher wurde vom TLfDI in Zusammenarbeit mit dem Apothekerverband auf das Problem aufmerksam gemacht und es wurden die datenschutzrechtlichen Bedenken erörtert und die Apotheker dafür sensibilisiert. Die Prüfung ist beim TLfDI jedoch noch nicht abgeschlossen.

10.20 Wearables und Gesundheits-Apps immer datenschutzkonform?

Einer repräsentativen Umfrage durch die Bitkom Research GmbH zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte deshalb in ihrer Entschließung im April 2016 „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ ihre Vorstellungen diesbezüglich veröffentlicht.

So weist die Konferenz darauf hin, dass zahlreiche Wearables und Gesundheits-Apps die aufgezeichneten Daten an andere Personen oder Stellen weiter geben, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Zudem müssen die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Dies sieht auch Artikel 25 der ab 25. Mai 2018 wirksam werdenden Datenschutzverordnung (DS-GVO) vor.

Zudem ist die Konferenz u. A. der Meinung, dass, wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in Umlauf bringt oder ihren Vertrieb systematisch unterstützt, eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt. Nicht zuletzt bezweifelt sie die Rechtmäßigkeit bei Einwilligungserklärungen etwa in Beschäftigungs- und Versicherungsverhältnissen (siehe Anlage 2).

Wearables und Gesundheits-Apps erfahren derzeit einen wirtschaftlichen Aufschwung. Dennoch muss jederzeit der Datenschutz gewährleistet sein. Eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt auch der Entwickler und der Betreiber solcher Angebote. Deshalb ist bereits in der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

10.21 Beschwerde über ein Reinigungsunternehmen wegen nicht korrekt vernichteter Nachweisblätter

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht, dass Nachweislisten eines Reinigungsunternehmens mit personenbezogenen Daten nicht datenschutzgerecht vernichtet und entsorgt würden.

Auf Nachfrage gab das Reinigungsunternehmen an, dass es mit der Nachweisliste die geleistete Dienstleistung dokumentiert und diese bei der Abrechnung nutzt. Die vor Ort tätigen Mitarbeiter führen die Listen, auf denen das Datum, die Uhrzeit und eine Kennnummer des Reinigungsobjekts notiert werden. Jede Reinigung wird einzeln mit einer Unterschrift abgezeichnet. Zu Abrechnungszwecken wird diese Liste dann digital eingelesen und die Papierbelege werden nach erfolgter Rechnungslegung in der Müllpresse entsorgt. Hierfür werden die Listen in Müllsäcken gesammelt, mit einem Kabelbinder verschlossen und in der Müllpresse verpresst.

Der TLfDI nahm zu diesem Ablauf Stellung und bemängelte, wie die Entsorgung der Nachweispapiere von-statten-geht, da sie personenbezogene Daten enthalten. Personenbezogene Daten sind nach § 3 Bundesdatenschutzgesetz (BDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Mit den auf der Nachweisliste aufgeführten Uhrzeiten und dem Namen des Mitarbeiters, könnte man nachverfolgen, wann sich die Person an welchem Ort aufgehalten hat. Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Vorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt

hat. Das Löschen ist auch eine Art der Verarbeitung. Gemäß § 3 Abs. 4 Nr. 5 BDSG ist das Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet worden sind und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Im vorliegenden Fall wäre das nach der Rechnungslegung.

Allerdings erfolgt hier keine Löschung. Bei einer datenschutzkonformen Löschung muss sichergestellt werden, dass die enthaltenen personenbezogenen Daten zerstört werden. Eine Müllpresse kann diese Anforderungen nicht erfüllen, da die Daten nachvollziehbar bleiben. Eine Unkenntlichmachung in Form von Schreddern der Listen ist notwendig, um diese datenschutzkonform zu löschen. Hinsichtlich der notierten Daten ist für die Vernichtung der Listen mindestens ein Schredder der Sicherheitsstufe P-3 entsprechend der DIN 66399 ausreichend. Das Unternehmen hat auf die Stellungnahme des TLfDI hin mitgeteilt, dass es zukünftig die Datenblätter datenschutzkonform entsorgen wird und hierzu eigens ein Schredder in der gewünschten Sicherheitsstufe angeschafft würde.

Personenbezogene Daten sind nach § 3 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person. Enthalten Dokumente personenbezogene Daten muss bei der Vernichtung darauf geachtet werden, dass sie unleserlich werden. Je nach Art der gespeicherten Daten muss hierfür ein Schredder mit der entsprechenden Sicherheitsstufe genutzt werden.

10.22 Urkundenverifikationsdienst Approbationsurkunden

Bereits im 11. Tätigkeitsbericht berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über den Einsatz einer Technik zur Verifikation von Approbationsurkunden von Ärzten und Fachkräften in Pflegeberufen. Es ging dabei darum, dass Patienten die Echtheit einer Approbationsurkunde eines Arztes prüfen können, ohne sich an die Landesärztekammer Thüringen wenden zu müssen. Das Verfahren läuft wie folgt ab: Seit 2016 stellt das Thüringer Landesverwaltungsamt Approbationsurkunden mit einem QR-Code versehen aus. Ein QR-Code (von Quick Response) ist ein zweidimensionales Bild, in dem bestimmte

Informationen hinterlegt sind. Diese können mithilfe eines sogenannten QR-Code-Scanners abgerufen werden, der beispielsweise als App auf das Smartphone geladen kann. Besitzer eines Smartphones können den QR-Code auf diesen „neuen“ Urkunden scannen, der einen 64-stelligen Code (Buschstaben und Zahlen) enthält, mit welchem jede Person mit Internetzugang auf dem Portal <https://www.kammerservice.de> unter Eingabe dieses Codes die Echtheit der Urkunde prüfen kann.



Bereits im letzten Tätigkeitbericht wurde berichtet, dass das Verfahren zur Generierung des 64-stelligen Codes den Datenschutzanforderungen entspricht. Im aktuellen Berichtszeitraum hatte der TLfDI weiterhin geprüft, wer Zugriff auf die Daten der Urkunden hat und wie diese vor Veränderung geschützt sind. Da die Landesärztekammer Thüringen, welche das Verifikationsportal mit anderen Ärztekammern in Deutschland betreibt, nicht die Stelle ist, die Urkunden selbst ausstellt, werden nur digitale Kopien des Urkundeninhalts bereitgestellt.

Wichtig aus datenschutzrechtlicher Sicht war, dass bei Übertragung der Kopien keine Datenveränderung durch Unbefugte (Hacker, böswillige Angestellte) stattfinden kann und das zum zweiten eine Sicherung der Daten gegen Zerstörung (auch hier durch Hacker bzw. technisches Versagen der Rechentechnik) gegeben ist.

Zum ersten Punkt der Sicherstellung der Integrität der Daten hat der TLfDI eine Lösung mit dem Thüringer Landesverwaltungsamt und der Landesärztekammer Thüringen abgestimmt und Verbesserungsvorschläge eingebracht, wie die zu übermittelnden Daten zusätzlich zum Übertragungsweg sicher verschlüsselt werden können. Zum zweiten Punkt (Schutz vor Datenverlust) trägt das Thüringer Landesverwaltungsamt die Verantwortung für die Richtigkeit der Urkundendaten. Hier muss dem TLfDI zurzeit noch ein schlüssiges Konzept zur Datensicherung nachwiesen werden.

Jede öffentliche Stelle bzw. nicht-öffentliche Stelle ist verpflichtet, beim Umgang mit personenbezogenen Daten in technischen Systemen die Daten vor unerlaubter Manipulation und vor Datenverlust zu schützen. Dabei kann es je nach Schutzbedarf der betroffenen Daten

erforderlich sein, nicht nur den Übertragungsweg bei einer Übermittlung zu verschlüsseln, sondern auch die Daten selbst.



Stempel 2 Datenschutz - © S. Engels / Fotolia.com

11 Ordnungswidrigkeiten

11.1 Bußgelder nehmen stetig zu

Wie in den vergangenen Tätigkeitsberichten dargestellt, ist der Thüringer Landesbeauftragte für den Datenschutz und die Informations-

freiheit (TLfDI) seit Übertragung der Zuständigkeit „Aufsichtsbehörde für den nicht-öffentlichen Bereich“ auch zuständige Ordnungswidrigkeitenbehörde für Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG).

Das Ordnungswidrigkeitenverfahren ist eine besondere Unterart des Verwaltungsverfahrens. Es ist streng von anderen Verfahren zu trennen. Im Unterschied zum grundsätzlich formfreien Verwaltungsverfahren handelt es sich um ein streng formalisiertes Verfahren mit vielen Parallelen zum strafrechtlichen Ermittlungsverfahren. Ziel des Verfahrens ist es, Verstöße gegen das Bundesdatenschutzgesetz zu ahnden und auf diesem Wege eine Änderung im Verhalten des Verstoßenden zu erreichen. Im Wesentlichen teilt sich die Befugnis des TLfDI in Ordnungswidrigkeiten wegen eines Verstoßes gegen Formalien des BDSG sowie gegen inhaltliche Verstöße auf. Erstere können mit einem Bußgeld bis zu 50.000 Euro, Letztere mit bis zu 300.000 Euro geahndet werden. Dabei wird die Höhe der Geldbuße durch die Bedeutung der Ordnungswidrigkeit und den Vorwurf, der den Täter trifft, bestimmt, aber bis zu einem gewissen Maße auch durch die finanzielle Leistungsfähigkeit des Täters. An die eben genannten Obergrenzen ist der TLfDI allerdings dann nicht gebunden, wenn der zu ahnende Verstoß einen finanziellen Vorteil erwirtschaftet hat, der über diese Obergrenzen hinausgeht. Dieser Vorteil kann dann ebenfalls abgeschöpft werden. Rechtswidriges Verhalten soll sich ja nicht lohnen.

Die Integration des Bußgeldverfahrens beim TLfDI ist abgeschlossen. Es wird aber immer noch daran gearbeitet, dessen Effizienz zu optimieren. Dies ist auch notwendig, weil der TLfDI in der Vergangenheit mit komplexen Verfahren konfrontiert war und in Zukunft bestimmt auch sein wird.

Während im letzten Berichtszeitraum Geldbußen in Höhe von insgesamt knapp über 13.000 Euro verhängt wurden, steigt dieser Betrag für diesen Berichtszeitraum auf über 45.000 Euro. Eine Entwicklung, die hinsichtlich des Datenschutzes auch mit Sorge beobachtet wird, da ein Grund hierfür schwere Verstöße waren, die mit hohen Bußgeldern geahndet werden mussten.

Schwerpunkt der Verfolgung waren die Nichtbestellung von betrieblichen Datenschutzbeauftragten trotz bestehender gesetzlicher Verpflichtung, § 42 Abs. 1 Nr. 2 BDSG, sowie unbefugtes Erheben oder Verarbeiten von personenbezogenen Daten nach § 43 Abs. 2 Nr. 2 BDSG.

Wird eine vorsätzliche Handlung, die nach § 43 Abs. 2 BDSG eine Ordnungswidrigkeit darstellt, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen, handelt es sich um eine Straftat. Diese zu verfolgen, ist der TLfDI nicht befugt. Vielmehr verfolgt die jeweils zuständige Staatsanwaltschaft die Tat auf Antrag. Neben dem Opfer und der verantwortlichen Stelle selbst, sind die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und auch der TLfDI in solchen Fällen antragsberechtigt.

Hiervon musste der TLfDI im Berichtszeitraum glücklicherweise nur einmal Gebrauch machen.

Ab Ende Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) in Europa und damit auch in Deutschland Geltung erlangen. Dies führt nicht nur zu Änderungen im Datenschutzrecht, sondern auch zu Änderungen bei den Bußgeldern. Die Bußgelder für formale Verstöße erhöhen sich auf 10.000.000 Euro, für materielle Verstöße auf 20.000.000 Euro!



Datenschutz - © Marco 2811 / Fotolia.com

12 Technischer und organisatorischer Datenschutz

12.1 Windows 10, Microsoft-Cloud Deutschland und Windows Office 365

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist per Gesetz durch das Thüringer Datenschutzgesetz (ThürDSG) verpflichtet, die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihrer Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, zu beobachten (§ 40 Abs. 5 ThürDSG). Gerade zu den oben genannten Themen erreichen den TLfDI auch Anfragen, und Reaktionen des TLfDI hierauf sollen kurz dargestellt werden:

Windows 10:

Für die Microsoft Deutschland GmbH ist die zuständige datenschutzrechtliche Aufsichtsbehörde das Bayerische Landesamt für Datenschutzaufsicht (BayLDA).

Da aber auch beim TLfDI Anfragen zum datenschutzgerechten Einsatz von Windows 10 eingingen, stellte der TLfDI im Juni 2016 eine kurze Handreichung auf seiner Website zur Verfügung (siehe https://www.tlfdi.de/mam/tlfdi/themen/windows_10.pdf).



Microsoft-Cloud Deutschland:

Die Microsoft Deutschland GmbH betreibt in Deutschland zwei deutsche Rechenzentren, mit der T-Systems, einer Tochter-Gesellschaft der Deutschen Telekom, als Datentreuhänder. Dies bedeutet, dass die T-Systems gegenüber dem Kunden vertraglich sicherstellt, dass Daten nicht Dritten offengelegt werden. Nach Angaben der T-Systems kann somit die Herausgabe der Daten nur der Kunde selbst verlangen oder auf einer deutschen Rechtsgrundlage beruhen. Nach derzeitigem Stand geht die T-Systems davon aus, dass somit ausländische Behörden keine Herausgabe der Daten verlangen können.

Ziel der Microsoft-Cloud Deutschland ist es, den Kunden dieser Cloud auf Wunsch hin anzubieten, dass die Daten in den Rechenzentren in Deutschland verbleiben.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder sind bezüglich der Microsoft-Cloud Deutschland derzeit im Gespräch, um datenschutzrechtliche Fragen zu klären. Siehe hierzu auch Nummer 2.1 des 13. Tätigkeitsberichts für den öffentlichen Bereich. Ein gemeinsamer Dialog wird sich sicherlich fortsetzen.

Microsoft-Office 365:

Der TLfDI als Vorsitzender des Arbeitskreises „Bildung und Datenschutz“ der unabhängigen Datenschutzbeauftragten des Bundes und der Länder prüft derzeit, ob Microsoft Office 365 für Schulen datenschutzgerecht einsetzbar ist.

Am Anfang bezog sich der Prüfungsbereich auf den Einsatzbereich im rein pädagogischen Kontext. Mittlerweile steht zudem die Frage im Raum, ob nicht auch Schulen für ihre eigene Verwaltung Microsoft Office 365 nutzen dürfen. Eine Antwort auf die letzte Frage interessiert natürlich auch Verwaltungen anderer öffentlicher und nicht-öffentlicher Stellen.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder beobachten weiterhin die Entwicklungen verschiedener

Microsoft-Produkte. Jegliche Anwendungen müssen zudem der DSGVO standhalten.

12.2 Kritische Infrastruktur – Sektor Gesundheit

Im Juni 2016 legten Kriminelle per Hackerangriff das Lukas-Krankenhaus in Neuss mit einer Erpresser-Botschaft lahm. Kaum ein Nachrichtenkanal berichtete nicht davon.

Schon lange sind IT-Systeme von Krankenhäusern derartigen Angriffen ausgesetzt, in letzter Zeit häufen sich derartige Attacken.

Nach einer Meldung des WDR traf es danach weitere Krankenhäuser, unter anderem das Klinikum Arnsberg.

Der Vorteil des Einzugs der digitalen Gesellschaft ist auch im medizinischen Bereich nicht von der Hand zu weisen. Aber mit dem Einzug dieser modernen Technik werden gleichzeitig auch neue Angriffspunkte ermöglicht.

Das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat zum Ziel, bei Kritischen Infrastrukturen die Sicherheit informationstechnischer Systeme zu erhöhen. Im April 2016 wurde dann eine BSI-Kritisverordnung (BSI-KritisV) in Kraft gesetzt, die die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation als Kritische Infrastrukturen einstuft, also Bereiche, deren Ausfall dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätte. Im Juni 2017 wurde die BSI-KritisV dann um die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr erweitert.

Somit sind nun auch Betreiber dieser Sektoren angehalten, IT-Sicherheit nach dem „Stand der Technik“ umzusetzen und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die BSI-Kritisverordnung (BSI-KritisV) regelt, welche Sektoren derzeit als Kritische Infrastruktur eingestuft sind. Bereits nach einem Jahr wurden die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr nachträglich aufgenommen, da diese 2016 einem hohen Gefährdungspotenzial ausgesetzt waren und deren Folgen bei Ausfall neu bewerten wurden.

12.3 Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung

Am 25. November 2009 beschlossen das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG unter anderem Änderungen über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Diese e-Privacy-Richtlinie, auch unter „Cookie-Richtlinie“ bekannt, regelt im Wesentlichen in Artikel 5 Absatz 3 die Verwendung von Cookies.

Die zusätzliche Richtlinie war damals ein Ergebnis der Überprüfung der Richtlinie 2002/58/EG („e-Datenschutz-Richtlinie“).

Entsprechend dem Erwägungsgrund 173 i. V. m. Artikel 95 der neuen Datenschutz-Grundverordnung (DS-GVO) sollte die Richtlinie 2002/58/EG nochmal einer Überprüfung unterzogen werden, sobald die DS-GVO angenommen wurde, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten.

Seit dem 10. Januar 2017 liegt nun ein Entwurf einer e-Privacy-Verordnung der Europäischen Kommission vor. Der Begründung zum Entwurf kann man entnehmen, dass seit der letzten Überprüfung der e-Datenschutz-Richtlinie im Jahr 2009 sich wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen haben. So heißt es: „Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen Entwicklung nicht Schritt gehalten, was zu einem mangelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führt.“

Weiterhin liefert der Entwurf der Verordnung die Begründung gleich mit, warum es nun eine Verordnung und keine Richtlinie werden soll: „Die Kommission legt einen Vorschlag für eine Verordnung vor, um die Kohärenz mit der Datenschutz-Grundverordnung (DS-GVO) sowie Rechtssicherheit gleichermaßen für Nutzer und Unternehmen dadurch zu gewährleisten, dass eine unterschiedliche Ausle-

gung in den Mitgliedstaaten vermieden wird. Eine Verordnung kann in der gesamten Union ein gleiches Schutzniveau für die Nutzer und niedrige Einhaltungskosten für grenzüberschreitend tätige Unternehmen sicherstellen.“

Geplant ist, dass die Verordnung, zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Ob der Termin gehalten werden kann, hängt stark davon ab, wie die einzelnen Gremien und betroffenen Wirtschaftsunternehmen Einfluss auf den Entwurf nehmen werden, denn die neuen Regelungen z. B. für das Online- und Direktmarketing, haben beträchtliches Diskussionspotenzial. Man erinnere sich daran, wie lange es gedauert hat, bis die DS-GVO verabschiedet wurde.

Auch die Artikel-29-Gruppe der EU-Datenschutzbeauftragten veröffentlichte ihre Kritikpunkte zum Entwurf der EU-Kommission. So dürften beispielsweise Analysen von Metadaten und Inhaltsdaten nur erfolgen, wenn alle Endnutzer ausdrücklich eingewilligt haben. Auch sieht die Artikel-29-Gruppe die allgemeinen Browsereinstellungen als Grundlage einer Einwilligung für Cookies als unzureichend an, da dies nicht der Informationspflicht gemäß Artikel 7 DS-GVO entspricht. Bezüglich des Trackings äußerte die Artikel-29-Gruppe z. B. Änderungswünsche dahingehend, dass Angebote von Websites oder Diensten nur erlaubt seien, wenn diese den Zugang auch ohne Tracking ermöglichen. Zudem ist sie der Meinung, dass bei WiFi- und Bluetooth-Tracking eine Information darüber nicht ausreiche, da die DS-GVO i. d. R. eine Einwilligung verlange.

Man wird abwarten müssen, welche Entwicklung der Entwurf der Verordnung noch nehmen wird.

Entsprechend Erwägungsgrund 173 i. V. m. Artikel 95 der Datenschutz-Grundverordnung, sollte, sobald die DS-GVO angenommen wurde, die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten. Geplant ist, dass die EU-e-Privacy-Verordnung zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Wird der Termin nicht gehalten, gelten für die Übergangszeit die DS-GVO und die e-Privacy-Richtlinie 2002/58/EG in Verbindung mit der jeweiligen nationalen Umsetzung.

12.4 Datenschleudern – vom vernetzten Auto

Vor einigen Jahren waren die Fahrzeuge nur reines Transportmittel, dessen Zweck es war, Personen von einem Ort zu einem anderen zu transportieren. Durch den Fortschritt in der digitalen Regelung und Steuerung zog zunehmend die Digitaltechnik auch in die Fahrzeuge ein. Heutzutage sind in Fahrzeugen zahlreiche Computersysteme verbaut, die die Funktion der einzelnen Komponenten überwachen (z. B. Bremsen, Motorsteuerung, Sitzverstellung, Entertainment-System, Navigationssystem) und Daten untereinander austauschen. Seit ca. 1970 können so Fehlerberichte über die einheitliche Schnittstelle OBD-II durch Werkstätten ausgelesen bzw. Speicher zurückgesetzt werden. Die Anzahl der berechtigten Personen, die Zugriff auf die generierten Daten besaßen, war im Regelfall überschaubar.

All dies ändert sich seit einigen Jahren.

Bereits im 10. Tätigkeitsbericht (2012/2013) berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit über das europäische Vorhaben, bordeigene eCall-Systeme in allen Fahrzeugen der Mitgliedstaaten verbindlich vorzuschreiben. Schon damals war erkennbar, dass in einer weiteren Ausbaustufe neben den Basisdaten zusätzliche Angaben hinzukommen werden, die z. B. Versicherungsgesellschaften, Kraftfahrzeug-Callcenter, Gesundheitsdienste, Rechtsanwälte oder Automobilclubs interessieren werden (siehe 10. Tätigkeitsbericht, Punkt 3.2). Entsprechend der EU-Verordnung 2015/758, müssen nun ab April 2018 alle Neuwagen mit eCall-Systemen ausgestattet werden. So bereitet sich die Wirtschaft seit Jahren darauf vor.

Durch das praktisch flächendeckend verfügbare Datennetz des Mobilfunks ist nun auch eine dauerhafte mobile Erreichbarkeit der Fahrzeuge gegeben.

Die Digitalisierung hat aber auch im Fahrzeug selbst Einzug gehalten. Laptops, Handys usw. können mit dem elektronischen Multimediacenter, sogenannte Infotainmentsysteme, im Fahrzeug bestens kommunizieren, fast so, als wäre man in einer modern ausgerüsteten Wohnstube auf vier Rädern. Wer kennt dies nicht? Steigt man in ein modernes Fahrzeug ein, kann man sich heutzutage schon oft mit mobilen Geräten, z. B. mit seinem Smartphone, mit dem Multimediacenter des Fahrzeuges verbinden und alle Kontakte des Smartphones vom Fahrzeug aus anrufen oder die auf dem Smartphone gespei-

cherte Musik oder Videos abspielen. Dabei werden die Telefonkontakte oft komplett auf das Multimediacentrum übertragen.

Vor einiger Zeit haben Hersteller wie Apple und Google sogar Möglichkeiten geschaffen, Apps das Smartphone vom Touch-Display des Fahrzeugs bedienen zu können. Ebenso bieten nun auch schon die Automobilhersteller eigene App-Anwendungen an. Moderne Infotainmentsysteme bieten bereits Apps auf herstellerspezifischen App-Stores an und erlauben die Individualisierung des Erlebnisses Autofahren. Viele Fahrzeuge bringen auch ihre eigene Datenverbindung ins Mobilfunknetz gleich mit und können somit z. B. direkt mit dem Fahrzeughersteller kommunizieren. Das zukünftige Fahrzeug wird also ein vernetztes Fahrzeug sein – bzw. ist es zum Teil schon heute. So komfortabel wie es ist, in den oben genannten Beispielen fallen große Mengen an Daten an. Also zum einen Daten über das Fahrzeug selbst und das Fahrverhalten, und zum anderen durch den Nutzer selbst, veranlasst aufgrund des Kontaktes zum Multimediacentrum. So fallen z. B. Daten an zur Motordrehzahl, Bremsverhalten, Beschleunigungsverhalten, Füllstand des Tanks, Ausschlag der Stoßdämpfer, Navigationszielen, aktuellem Standpunkt und aktueller Geschwindigkeit, Fahrtrichtung, Insassenzahl, Kamerabildern von Rückfahrt- und Frontkameras, Abstandssensoren usw. – die Liste ließe sich noch lange fortsetzen. Zum anderen können evtl. auch Daten von Nutzern erfasst werden, die sich in diesem Fahrzeug befinden und mit ihren Geräten mit dem Multimediacentrum gewollt oder nicht gewollt in Kontakt stehen (z. B. indem Verbindungen gespeichert werden oder Gerätekennungen auch bei nichtaktiver Verbindung ausgelesen werden).

Das Problem ist, dass viele dieser Daten einen „Personenbezug“ aufweisen und durch ihre Analysen sogar ein Verhaltensprofil erstellt werden kann. Aus den Daten kann beispielsweise der Fahrstil des Fahrers (und dessen Risikobereitschaft), die Übertretung von Verkehrsregeln und natürlich auch der Verlauf von Aufenthaltsorten, wie z. B. die Route des letzten Urlaubs oder der Dienstreisen, ermittelt werden.

Die Versicherungsbranche und auch die Wirtschaft sehen bereits seit Jahren ein großes Marktpotential bezüglich der Auswertung solcher Daten. Ihre Geschäftsmodelle und die Wertschöpfung werden sich im Rahmen der digitalisierten Fahrzeuge zukünftig enorm auf den digitalen Mobilitätsbereich erweitern. Die vom Bundesministerium für Verkehr und digitale Infrastruktur veröffentlichte Studie „Eigen-

tumsordnung“ für Mobilitätsdaten“ vom August 2017 gibt einen ersten Eindruck, wohin die Reise zukünftig gehen könnte (siehe

<http://www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html>).



So gilt es beispielsweise dringend zu klären, welche Daten überhaupt erforderlich sind, wem eigentlich die in einem Fahrzeug anfallenden Daten gehören, wer also „Eigentümer“ (oder Verfügungsberechtigter) dieser Daten und somit auch datenschutzrechtlich verantwortlich für diese ist, und wer sie wann nutzen darf.

Ab dem 25. Mai 2018 tritt zudem die Europäische Datenschutz-Grundverordnung (DS-GVO) in Kraft. So regelt beispielsweise Artikel 25 DS-GVO, dass Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden müssen (Data protection by design) und IT-Systeme datenschutzfreundlich so voreingestellt sein müssen, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

Auch auf die zukünftige Umsetzung des Artikels 6 DS-GVO, Rechtmäßigkeit der Verarbeitung, darf man gespannt sein. Die Erfassung und Weitergabe der Daten bedürfen immer einer Erlaubnisnorm oder einer Einwilligung. Auch das „Recht auf Vergessenwerden“ (Artikel 17 DS-GVO) oder das Auskunftsrecht über die betreffenden Daten (Artikel 20 DS-GVO), ist umzusetzen. Man darf gespannt sein, insbesondere bei Carsharing-Lösungen.

Es gibt also noch viel zu tun, damit Daten in Fahrzeugen datenschutzgerecht verarbeitet werden. Wünschenswert ist dabei u. A., dass Fahrzeughalter oder Fahrzeugnutzer grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahrzeugdaten selbst entscheiden können.

So weist auch die vom Bundesministerium für Verkehr und digitale Infrastruktur eingesetzte „Ethik-Kommission zum automatisierten Fahren“ in ihrem Bericht vom Juni 2017 daraufhin, dass Geschäftsmodelle, die sich diese anfallenden Daten zunutze machen, ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer finden. Fahrzeughalter oder Fahrzeugnutzer sollten grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahr-

zeugdaten entscheiden können. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, so die Ethik-Kommission, sollte frühzeitig entgegengewirkt werden. Weiterhin führt die Ethik-Kommission in ihren 20-Ethik-Leitlinien aus, dass klar unterscheidbar sein muss, ob ein fahrerloses System genutzt wird oder ein Fahrer mit der Möglichkeit des „Overrulings“ Verantwortung behält. Dabei muss bei nicht fahrerlosen Systemen die Mensch/Maschine-Schnittstelle so ausgelegt werden, dass zu jedem Zeitpunkt klar geregelt und erkennbar ist, welche Zuständigkeiten auf welcher Seite liegen, insbesondere auf welcher Seite die Kontrolle liegt. Für die dazu notwendige Protokollierungs- und Dokumentationspflicht ist eine internationale Standardisierung anzustreben.

Auch die 39. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre forderte in ihrer Entschließung vom 25. bis 29. September 2017 die Hersteller, Behörden und Anbieter fahrzeugbezogener Dienste auf, u. A.

- sichere Datenspeicher bereitzustellen, um Zugriffe steuern zu können,
- Technologien zu entwickeln, die unzulässige Zugriffe und das Mitschneiden von persönlichen Daten bei Fahrzeugen, Infrastrukturen und Einrichtungen verhindern,
- technische Maßnahmen bereitzustellen, die Cyberangriffe verhindern,
- die Datensparsamkeit zu beachten und die Datenlöschung nach einer gewissen Zeit zu gewährleisten und z. B. auch
- eine Datenschutz-Folgeabschätzung für neue, innovative oder riskante Entwicklungen durchzuführen.

Mobilität 4.0, so wird die Digitalisierung der Mobilität oft genannt, um den Komfort und die Verkehrssicherheit zu erhöhen, darf nicht auf Kosten des Rechts auf informationelle Selbstbestimmung gehen. Dieses Recht ist ein Grundrecht gemäß Artikel 2 Abs. 1 i. v. m. Art. 1 Abs. 2 Grundgesetz.

Die Ethik-Kommission weist zu Recht darauf hin, dass auch datenschutzfreundliche Innovationen (Privacy by Design) gefördert werden müssen. Es gilt eben auch zu verhindern, dass z. B. im Rahmen einer zentralen Verkehrssteuerung und der Erfassung aller Kraftfahr-

zeuge, es zu einer Totalüberwachung aller Verkehrsteilnehmer kommt.

Aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist es deshalb wichtig, Gelegenheiten zu nutzen, um mit der Auto-Industrie, Politikern und anderen Interessenten in Kontakt zu treten. So nutzte der TLfDI z. B. in Augsburg, Jena und Bielefeld die Möglichkeit, datenschutzrechtliche Hinweise zu geben und datenschutzrechtliche (Fehl-) Entwicklungen zu finden.

Moderne Fahrzeuge werden in naher Zukunft vollständig vernetzt sein. Die anfallenden Daten werden zukünftig Begehrlichkeiten verschiedener Wirtschaftszweige wecken. Die möglichen Daten haben das Potenzial der Verhaltenskontrolle und verraten viel über den Fahrer. Deshalb sind bei der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

12.5 Pflichten sozialer Netzwerke

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigten sich schon recht früh mit der datenschutzrechtlichen Thematik von sozialen Netzwerken. Durch Facebook aber mit seinen mächtigen Funktionen, die so viel Daten wie möglich sammeln, um dem Nutzer ein „optimales“ Angebot bereitstellen zu können, wurde eine neue Qualität von sozialen Netzwerken geschaffen. Mit der Idee der „optimalen Kundenbetreuung“ ging zwangsweise die Notwendigkeit einer umfassenden Profilbildung der Nutzer einher. Nach dem Motto: Je mehr ich von einem Nutzer weiß, umso besser kann ich durch Algorithmen geschäftsmäßig die Bedürfnisse der Wirtschaft mit dem Kunden verbinden, auch die eigenen.

So stellte im September 2011 die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder u. a. klar, dass sich Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben (siehe

https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/80/82_nutzerdaten.pdf).

In den meisten sozialen Netzwerken werden auch Funktionen angeboten, die es ermöglichen, mit anderen Leuten zu diskutieren, Beiträge, Fotos und Videos zu teilen. Somit können Anbieter sozialer Netzwerke durch deren Inhalte und Kommunikationspartner den Nutzer anhand seiner hinterlassenen Daten noch genauer analysieren. Diese Kommunikationsmöglichkeiten haben aber in den letzten Jahren eine besondere Dynamik erlangt. Neben Cybermobbing und anderen strafbaren Inhalten ist zunehmend eine Verbreitung von Hasskriminalität in den sozialen Netzwerken zu verzeichnen. Facebook z. B. verkündete im Mai 2017, dass nun tausende Mitarbeiter eingestellt würden, um dem entgegenzuwirken. Doch wie will man die Millionen Beiträge täglich überprüfen? Was ist zudem strafbar und was ist Kunst oder Meinungsfreiheit? Fast denkt man hier an Goethes Zauberlehrling und die Geister, die man selber rief.

In Deutschland gilt nun seit dem 1. Oktober 2017 das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Bundesgesetzblatt Nr. 61 vom 7. September 2017).

Durch dieses Netzwerkdurchsetzungsgesetz (NetzDG), sollen die Hasskriminalität und andere strafbare Inhalte in sozialen Netzwerken minimiert werden. So sind Anbieter sozialer Netzwerke nun verpflichtet, bei einem offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde diesen zu entfernen oder den Zugang zu ihm zu sperren. Dies gilt nicht, wenn der Anbieter mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat.

Handelt es sich um einen rechtswidrigen Inhalt, dessen Offensichtlichkeit nicht gleich erkennbar ist, muss der Anbieter trotzdem in der Regel innerhalb von sieben Tagen die Löschung oder Sperrung durchführen. Diese Zeit verlängert sich, falls der Anbieter zwecks Entscheidungsfindung über die Rechtswidrigkeit des Inhalts z. B. dem Nutzer vor der Entscheidung Gelegenheit zur Stellungnahme zu der Beschwerde gibt.

Falls es zu einer Löschung kommt, hat der Anbieter des sozialen Netzwerks, den Inhalt für die Dauer von zehn Wochen zu speichern. Weiterhin sind der Beschwerdeführer und der Nutzer über jede Ent-



scheidung unverzüglich zu informieren und die Entscheidung ist zu begründen.

Kritiker sehen hier eine Lücke, da nur eine Informationspflicht vorliegt. Ein Widerspruchsrecht für die Nutzer gibt es nicht.

Hat der Anbieter vom sozialen Netzwerk diesbezüglich mehr als 100 Beschwerden im Kalenderjahr, so ist er berichtspflichtig. Der deutschsprachige Bericht ist auf seiner Homepage und im Bundesanzeiger entsprechend dem NetzDG zu veröffentlichen.

Im Übrigen gelten die Regelungen zu den Beschwerden und zur Berichtspflicht nicht für Anbieter sozialer Netzwerke, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

Anbieter sozialer Netzwerke, die auf den europäischen Markt zielen, müssen sich auch dann an europäische Datenschutzstandards halten, wenn sie ihren Sitz außerhalb Europas haben. Zudem gilt es ab dem 1. Oktober 2017 das Netzwerkdurchsetzungsgesetz (NetzDG) zu beachten.

12.6 Google-Analytics

Im 9. Tätigkeitsbericht (TB) des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde auf die Möglichkeit des datenschutzgerechten Einsatzes von Google Analytics hingewiesen. So wurde berichtet, dass die Voraussetzung hierfür die Löschung des letzten Oktetts der IP-Adresse und ein Widerspruch gegen die Erfassung von Nutzungsdaten mittels eines von Google bereitgestellten Deaktivierungs-Add-On durch den Nutzer notwendig ist. Neben diesen umzusetzenden Parametern muss der Website-Betreiber, um einen datenschutzgerechten Betrieb von Google Analytics zu ermöglichen, zudem schriftlich einen Vertrag zur Auftragsdatenverarbeitung mit Google Inc. abschließen. Ein Muster dieses Vertrages wird von der Google Inc. selbst auf deren Website bereitgestellt (siehe 9. TB, Pkt. 4.1).

Aufgrund der Tatsache, dass das Safe-Harbor-Abkommen vom Europäischen Gerichtshof am 6. Oktober 2015 für ungültig erklärt wurde, prüfte der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit (HmbBfDI) als zuständige Aufsichtsbehörde erneut den Mustervertrag. Nach Aussagen des HmbBfDI hat die Google Inc. die Zertifizierung nach dem aktuellen EU-US-Privacy-

Shield durchgeführt und somit die rechtlichen Voraussetzungen auch für die Erbringung des Dienstes Google-Analytics im Wege der Auftragsdatenverarbeitung geschaffen.

Hinweise zum aktuellen Mustervertrag zur Auftragsdatenverarbeitung sowie aktuelle Hinweise zum datenschutzgerechten Einsatz von Google-Analytics finden Sie auf der Website:

https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf



Der Einsatz von Google-Analytics ist aus datenschutzrechtlicher Sicht nur unter bestimmten Voraussetzungen erlaubt. Hinweise hierzu finden Sie auf der Website der zuständigen Aufsichtsbehörde.

12.7 Speicherung von IP-Adressen – Sicherheit oder Datenschutz?

Ob dynamische oder statische IP-Adressen personenbezogene Daten im Sinne des Datenschutzrechtes sind oder nicht, darüber urteilen, seitdem es Websites gibt die jeweiligen Gerichte in den einzelnen Bundesländern recht unterschiedlich. Die Datenschutzbeauftragten des Bundes und der Länder standen aus ihrer Sicht dabei immer auf dem Standpunkt, dass statische IP-Adressen personenbezogen sind und zumindest bei dynamischen IP-Adressen u. U. ein Personenbezug herstellbar sei. Aber unter den jeweiligen Gerichten in den Bundesländern gab es hierzu keine einheitliche Rechtsauffassung.

So muss man fast von Glück reden, dass es eine Klage in dieser Sache vor ein paar Jahren bis zum Bundesgerichtshof (BGH) geschafft hatte. Herr Patrick Breyer, Parteimitglied der Piraten-Partei, hatte vor vielen Jahren geklagt, dass Einrichtungen des Bundes seine Internetprotokoll-Adressen (IP-Adressen) beim Zugriff auf ihre Websites aufzeichnen und speichern. Das Amtsgericht Tiergarten wies die Klage 2008 ab (AZ 2 C 6/08), wogegen Herr Breyer Berufung einlegte. Gegen das nachfolgende Urteil aus dem Jahr 2013 vom Landgericht Berlin wurde Revision eingelegt, sodass es beim BGH landete.

Der BGH entschied in seinem Beschluss vom 28. Oktober 2014 (Beschl. v. 28.10.2014, Az. VI ZR 135/13), das Verfahren auszusetzen und den Europäischen Gerichtshof (EuGH) zwecks Klärung zweier Fragen zu bitten.

Dabei war entsprechend der Informationen des EuGH Folgendes zu klären:

- 1.) Ob in diesem Zusammenhang auch „dynamische“ IP-Adressen für den Betreiber der Website personenbezogene Daten darstellen, sodass sie den für solche Daten vorgesehenen Schutz genießen. Eine „dynamische“ IP-Adresse ist eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert. Anders als statische IP-Adressen erlauben dynamische IP-Adressen es nicht, anhand allgemein zugänglicher Dateien eine Verbindung zwischen einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen. Somit verfügt ausschließlich der Internetzugangsanbieter von Herrn Breyer über die zu dessen Identifizierung erforderlichen Zusatzinformationen.
- 2.) Ferner wollte der BGH wissen, ob der Betreiber einer Website zumindest grundsätzlich die Möglichkeit haben muss, personenbezogene Daten der Nutzer zu erheben und zu verwenden, um die generelle Funktionsfähigkeit seiner Website zu gewährleisten. Der BGH wies insoweit darauf hin, dass die einschlägige deutsche Regelung von der deutschen Lehre überwiegend dahin ausgelegt werde, dass die Daten am Ende des jeweiligen Nutzungsvorgangs zu löschen seien, soweit sie nicht für Abrechnungszwecke benötigt würden.

Zwei Jahre später, am 19. Oktober 2016, entschied der EuGH über diese zwei Fragen (Rechtsache C-582/14):

Zu 1.) Eine dynamische Internetprotokoll-Adresse stellt ein personenbezogenes Datum für den Website-Anbieter dann dar, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.

Dies bedeutet, er muss rechtlich die Möglichkeit haben, den Internetzugangsanbieter zwecks Zusatzinformationen abfragen zu dürfen. Diese Möglichkeit besteht beispielsweise im Fall von „Cyberattacken“, bei dem ein Strafverfahren eingeleitet werden kann.

Zu 2.) Eine Regelung eines Mitgliedstaats, wonach IP-Adressen nur zu Abrechnungszwecken längerfristig gespeichert werden dürfen, sei

in Bezug auf Art. 7 Buchstabe f der europäischen Datenschutz-Richtlinie europarechtswidrig. Eine nationale Regelung darf nicht die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließen, indem sie für diese Kategorien das Ergebnis der Abwägung abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt. Daher stellt sich die Frage, ob § 15 Telemediengesetz (TMG) richtlinienkonform dahin ausgelegt werden muss, dass bei der Sicherstellung der Funktion des Telemediums über die Nutzungsdauer hinaus personenbezogene Daten Verwendung finden dürfen, soweit und solange die Verwendung zu diesem Zweck erforderlich ist.

Am 15. Mai 2017 traf dann der BGH, aufgrund der Einschätzung des EuGH, folgende Entscheidung (VI ZR 135/13):

Zu 1.) Die dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum dar.

Zu 2.) § 15 Abs. 1 TMG ist nun dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

Allerdings sieht der BGH diese notwendige Abwägung im Streitfall beim Landgericht Berlin nicht geprüft. Für diese Abwägung sind vor allem das Angriffsrisiko auf Anbieterseiten sowie die Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht des Nutzers entscheidend.

Der BGH verwies den Fall schließlich wieder zurück an das Landgericht Berlin.

Dynamische IP-Adressen stellen ein personenbezogenes Datum dar. § 15 Abs. 1 Telemediengesetz ist dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle

Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

12.8 eIDAS – was ist das?

Im 11. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit wurde unter der Überschrift „eIDAS – was ist das?“ über die eIDAS-Verordnung berichtet. Es ging darum, dass mit der am 23. Juli 2014 verabschiedeten EU-„Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben wurde. Diese Verordnung wird eIDAS-Verordnung genannt (electronic identification and trust services) und ist unmittelbar geltendes Unionsrecht.

Die Vorschriften bezüglich der Vertrauensdienste traten allerdings erst ab dem 1. Juli 2016 in Kraft. Vertrauensdienste definiert die eIDAS-Verordnung in Artikel 3 wie folgt: Ein Vertrauensdienst ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten anbietet. Vertrauensdienste sind aber auch Dienste, die die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder die Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten, anbietet.



Vertrauensdiensteanbieter können ihre Dienste/Produkte auch zu einem „qualifizierten Dienst“ zertifizieren lassen und dürfen dann ihre Dienste mit dem neuen EU-Vertrauenssiegel bewerben. Um der eIDAS-Verordnung bezüglich der Vertrauensdienste gerecht zu werden, trat in Deutschland am 29. Juli 2017 das eIDAS-Durchführungsgesetz mit zahlreichen Gesetzesänderungen in Kraft (BGBl. Nr. 52/2017). Mit dem darin enthaltenen neuen Vertrauensdienstegesetz (VDG) wurde die wirksame Durchführung der Vorschriften über Vertrauensdienste rechtlich geregelt.

Zuständige Aufsichtsstelle für Vertrauensdienste im Bereich der Erstellung, Überprüfung und Validierung von Zertifikaten für Website-Authentifizierung ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). Für die Aufgaben der anderen Bereiche ist die Bundesnetzagentur (BNetzA) zuständig.

Mit dem eIDAS-Durchführungsgesetz wurden zudem das Signaturgesetz und die Signaturverordnung außer Kraft gesetzt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen nun zeitnah aktualisiert werden. Entsprechend der Übergangsvorschrift werden zudem die von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Entsprechende akkreditierte Zertifizierungsdiensteanbieter müssen also rechtzeitig neue Zertifikate beantragen.

Mit Inkrafttreten des Vertrauensdienstegesetzes am 29. Juli 2017 werden alle von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen zudem nun zeitnah überarbeitet werden.

12.9 EU- und nationale Cybersicherheit

Am 5. Juli 2016 veröffentlichte die EU-Kommission eine Mitteilung unter der Überschrift „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“. Der Mitteilung war zu entnehmen, dass einer Untersuchung zufolge mindestens 80 Prozent der europäischen Unternehmen im Jahr 2015 zumindest einmal mit einem Cybervorfall zu tun gehabt haben. Zudem nahm die Zahl der Sicherheitsvorfälle in der gesamten Wirtschaft 2015 weltweit um 38 Prozent im Vergleich zum Vorjahreszeitraum zu.

Die Europäische Kommission will deshalb eine verstärkte Zusammenarbeit sowohl über Ländergrenzen hinweg als auch zwischen allen Akteuren und allen Sektoren, die im Bereich der Cybersicherheit aktiv sind, fördern. Außerdem will sie dazu beitragen, dass in der EU innovative und sichere Technologien, Produkte und Dienste entwickelt werden.

Diese Mitteilung ist im zeitlichen Kontext der Maßnahmen zu sehen, die die Cybersicherheit in Europa erhöhen sollen. Denn am Tag darauf, am 6. Juli 2016, verabschiedete das Europäische Parlament die „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, kurz auch NIS-Richtlinie genannt (Richtlinie (EU) 2016/1148 vom 6. Juli 2016, [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/DE/TEXT/PDF/?uri=CELEX:32016L1148&from=DE)



[content/DE/TEXT/PDF/?uri=CELEX:32016L1148&from=DE](https://eur-lex.europa.eu/legal-content/DE/TEXT/PDF/?uri=CELEX:32016L1148&from=DE)).

Die Mitgliedstaaten der EU müssen dem nun Rechnung tragen und die Bestimmungen der NIS-Richtlinie in nationales Recht umsetzen. Die so getroffenen Vorschriften und Umsetzungsmaßnahmen sind bis zum 9. Mai 2018 der Kommission mitzuteilen. Etwaige spätere Änderungen sind dann immer unverzüglich der Kommission zu melden.

Die Bundesrepublik Deutschland hat deshalb ein Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 beschlossen. Dieses Gesetz ist vom 23. Juni 2017 und im Bundesgesetzblatt Nr. 40 von 2017 veröffentlicht. Es ist als „Gesetz zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-Richtlinien-Umsetzungsgesetz) am 30. Juni 2017 in Kraft getreten.

Das Gesetz ist ein sogenanntes Artikel-Gesetz und regelt in einzelnen Artikeln die Änderungen von verschiedenen, nachfolgend aufgeführten Gesetzen. So wurden das BSI-Gesetz (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Energiewirtschaftsgesetz (EnWG), das Atomgesetz (AtG) und auch das Fünfte Buch des Sozialgesetzbuches in Teilen angepasst.

Gemäß BSIG müssen beispielsweise die Betreiber Kritischer Infrastrukturen ihre IT-Sicherheit nach dem „Stand der Technik“ umsetzen und deren Einhaltung regelmäßig gegenüber dem BSI nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im

Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.^a

Im TKG werden Telekommunikationsanbieter sowie auch im TMG Telemediendiensteanbieter nunmehr dazu verpflichtet, IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ zu ergreifen und zu erhalten, die nicht nur dem Schutz personenbezogener Daten dienen, sondern auch dem Schutz vor unerlaubten Eingriffen in die Infrastruktur.^b

Bezüglich der Telekommunikationsnetze erweitert sich die bereits bestehende Meldepflicht gemäß § 109 Absatz 5 TKG insofern, dass Beeinträchtigungen sowohl an die Bundesnetzagentur als auch an das BSI gemeldet werden müssen. Betreiber Kritischer Infrastrukturen gemäß BSI-Kritisverordnung müssen ebenfalls eine Kontaktstelle beim BSI registrieren.

Wichtigste Änderung im Energiewirtschaftsgesetz (EnWG) ist die Tatsache, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Meldepflicht von IT-Störungen auf alle Energieversorgungsnetzbetreiber ausgeweitet hat. Letztere müssen hierfür eine zuständige Kontaktstelle einrichten.

Beim Atomgesetz (AtG) ist dies für die Betreiber gleichlautend formuliert.^c

Zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit haben Mitgliedstaaten der EU die seit 2016 in Kraft gesetzte EU-NIS-Richtlinie in nationales Recht umzusetzen. Bis zum 9. Mai 2018 sind die getroffenen Vorschriften und Maßnahmen der Europäischen Kommission zu melden.

12.10 Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)

Wie bereits an anderer Stelle erwähnt, arbeiten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder themenbezogen bundesweit in sehr vielen Arbeitskreisen und Unterarbeitsgruppen

^a weitere Details vgl.

https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_IT_SiG/neur_IT_SiG_node.html

^b ebenda

^c ebenda

zusammen. Darüber hinaus gibt es auch internationale Arbeitsgruppen.

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) finalisierte im April 2016 das Arbeitspapier „Aktualisierung zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien“. Das Arbeitspapier spricht diesbezügliche Empfehlungen aus, die an verschiedene Akteure gerichtet sind, so auch an die Gesetzgeber, bestehende Regelungslücken zu schließen.

Im November 2016 wurde von der internationalen Arbeitsgruppe das „Arbeitspapier zu Biometrie in der Online-Authentifizierung“ verabschiedet. Oft wird der Zugang zur Hard- oder Software schon per Fingerabdruck oder Gesichtserkennung ermöglicht. Aber auch bei dieser Methode müssen Datenschutz und Datensicherheit sichergestellt sein.

Im April 2017 wurde dann das „Arbeitspapier zum Thema E-Learning-Plattformen“ fertiggestellt. Mit dem zunehmenden Einsatz von E-Learning-Plattformen wächst die Menge an personenbezogenen Daten, die über die Lernenden zur Verfügung stehen. Diese Daten könnten beispielsweise zu Prognosen des geistigen Zustands herangezogen werden und gewollte oder ungewollte lebenslange Schlussfolgerungen nach sich ziehen. Betreiber solcher Plattformen tragen hier eine sehr hohe datenschutzrechtliche Verantwortung.

Alle drei Arbeitspapiere sind auf der Seite der internationalen Arbeitsgruppe abrufbar <https://www.berlin-privacy-group.org>.



Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat die Arbeitspapiere zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien, zu Biometrie in der Online-Authentifizierung und zum Thema E-Learning-Plattformen veröffentlicht.

12.11 Wenn Kühlschränke eiskalt angreifen

Das ist keine Utopie mehr. Im Herbst 2016 mussten in den USA viele Menschen rund zwei Stunden ohne Musik von Spotify und

Soundcloud, ohne Twitter, ohne Netflix und ohne ein Dutzend anderer beliebter Onlinedienste auskommen.

Was war geschehen?

Zunehmend halten Haushaltsgeräte im privaten Bereich Einzug, die internetfähig sind. Sie haben neben einer IP-Adresse eine Software, die nicht vom Kunden überschaubar bzw. kontrollierbar ist. Dies betrifft z. B. Kühlschränke, Thermostate, Videogeräte, hausinterne Webcams usw.

Oft werden diese Geräte zudem mit Standard-Administrations-Passwörtern ausgeliefert, deren Änderung für den Normalverbraucher schon eine Hürde darstellt.

Hacker haben dies bereits erkannt, schalten sich auf solche Geräte auf, programmieren sie so, dass diese zu einem bestimmten Zeitpunkt zeitgleich einen Angriff ausüben. Also zur gleichen Zeit festgelegte Ziel-Server mit Anfragen zuschütten, sodass die Server dann überlastet sind. Im Fachbereich spricht man von einem Botnetz, welches solche Angriffe ausführt.

Nun mag man denken, so etwas wird nicht in Deutschland geschehen. Im November 2016 wurde aber eine größere Anzahl von Routern der Telekom, die unzählige Haushalte vor Angriffen schützen sollten, selbst Opfer eines Hackerangriffes. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) waren dabei über 900.000 Kundenanschlüsse betroffen. Nach Angaben der Telekom handelte es sich dabei um Telekom-Router von Drittanbietern. Ziel des Angriffs war die Installation einer Schadsoftware auf diese Router, damit diese dann als Teil eines sogenannten Botnetzes fungierten, also als fernsteuerbare Infrastruktur für weitere Angriffe zur Verfügung stehen. Nach Angaben der Telekom war die Installation der Schadsoftware bei denen, die die Telekom betrieb, nicht erfolgreich. Bei dem Versuch, die Schadsoftware zu installieren, stürzten diese aber ab. So war für viele Kunden kein Internet und keine IP-Telefonie möglich. Der Angriff auf die Drittanbieter-Router diente der Konstruktion eines Botnetzes zum gleichzeitigen Angriff auf externe Server.

Was ist aber, wenn zukünftige Angriffe nicht nur externen Servern gelten, sondern internetfähige Geräte im Haushalt das Ziel solcher Angriffe sind? Also Router gekapert werden, um Geräte innerhalb des Hauses zu manipulieren, auch um diese für Großangriffe fit zu machen?

Was passiert eigentlich zukünftig, wenn auch hier Hacker Kühlschränke eiskalt manipulieren? Welche Folgen ergeben sich zukünftig für den Bürger daraus? Wird dann der komplette digitalisierte Haushalt von staatlicher Seite abgeschaltet, sämtliche Geräte im Haushalt, einschließlich PC und Smartphone, überprüft? Gibt es dann noch Fernsehen und Strom, da auch diese Geräte mittlerweile vernetzt sind? Welche Rechte und Pflichten wird zukünftig der Bürger in der digitalen Gesellschaft haben?

Wenn große Unternehmen sich schon nicht vor Hackerangriffen schützen können, ist es nur eine Frage der Zeit, wann auch in Deutschland beispielsweise Kühlschränke eiskalt angreifen.

Der Einzug in die digitale Gesellschaft kommt und ist auch richtig, nur bedarf es auch einer digitalen und dementsprechenden technischen und rechtlichen Sicherheit für die Bürger, die von den jeweiligen Herstellern solcher Geräte zukünftig sichergestellt werden muss. Die Hersteller von internetfähigen Geräten und auch der Rechtsstaat müssen sich langfristig der Verantwortung bewusst werden, dass die Einführung der digitalen Gesellschaft nicht auf Kosten der Bürger und ihrer Grundrechte gehen darf.

Der TLfDI stellt hierfür seine Erfahrungen und Kenntnisse gern bereit.

Hersteller von internetfähigen Geräten müssen für ihr Produkt haftbar gemacht werden. Geräte sind zudem so zu gestalten, dass neben eindeutigen und verständlichen Hinweisen der Hersteller für Käufer beispielsweise schon beim Erwerb eines solchen Gerätes mit einfachen Mitteln das jeweilige Standard-Passwort vom Eigentümer geändert werden kann.

12.12 Canvas-Fingerprinting

Zunehmend werden bei der Darstellung von Websites Browser-Fingerprints verwendet, um Internetnutzer zu tracken, um so z. B. personalisierte Werbung zu schalten. Fingerprinting ist eine Methode, um Hersteller und Versionen von Software-Anwendungen über ein Netzwerk zu erkennen, obwohl diese Informationen nicht explizit vom System kommuniziert werden. Die Methode erlaubt es, auf Cookies oder Logins zu verzichten. Canvas-Fingerprinting ist eine solche Methode.

Wie funktioniert Canvas-Fingerprinting? Beim Aufruf einer Website werden von der Website im Hintergrund Informationen über bestimmte Software- und Hardware Merkmale ermittelt, die der Browser selbst bei Aufruf zwecks optimaler Darstellung mitliefert oder auf Anfrage nachliefert. Diese Informationen werden bei Canvas-Fingerprinting erfasst, indem sozusagen kleine Grafiken „gezeichnet“ werden. Jede Konfiguration von Hard- und Software erstellt die Grafiken mit leichten Abweichungen zueinander. Diese werden dann zur Identifizierung genutzt. Die so gesammelten Daten, wie beispielsweise der Browsertyp und Version, genutzte Schriftart, installierte Schriftarten, Bildschirmgröße, Sprache, die Art des Grafikprozessors usw., geben Aufschluss über das jeweilige Gerät. Über die gesammelten Daten entsteht somit der o. g. „Fingerabdruck“ (engl.: Fingerprinting) des jeweiligen technischen Gerätes. Je mehr Daten für die Bildung des Fingerabdrucks erfasst werden, umso genauer ist dieser Fingerabdruck und somit der Wiedererkennungswert des Gerätes.

Man kann sich vor Canvas-Fingerprinting schützen, indem man Java-Script in den Browsereinstellungen deaktiviert. Der Nachteil davon ist, dass dann allerdings viele Anzeigen von Webseiten nicht mehr richtig funktionieren. Auch empfehlen IT-Experten, mindestens zwei bis drei verschiedene Browser für verschiedene Suchanfragen zu verwenden. Dies erscheint für normale Nutzer zu umständlich. Weitere IT-Experten empfehlen, Anonymisierungsnetzwerke wie TOR zu nutzen. Letzteres zieht aber nur eine Anonymisierung des Netzverkehrs nach sich – die Inhalte, welche zur Identifikation herangezogen werden, werden durch TOR nicht anonymisiert. Für das tägliche Surfen erscheint dies auch ein umständlicher Weg. Manche Browser bieten auch schon Canvas-Blocker an. Solch ein Canvas-Blocker als sogenanntes Add-on kann Zugriffe auf Canvas-Elemente blockieren. In den Einstellungen des Add-on kann man dann das gewünschte Verhalten konfigurieren. Dieses Add-on sollte aber nur von der Online-Plattform des jeweiligen Browserherstellers geladen werden.

Es gibt demnach durchaus verschiedene Möglichkeiten, sich zu schützen. Jeder muss für sich selbst entscheiden, welchen Weg er gehen möchte.

Zunehmend werden bei der Darstellung von Websites heimlich Browser-Fingerprints verwendet, um Internetnutzer zu tracken. Da-

mit kann z. B. personalisierte Werbung geschaltet werden. Die beschriebene Methode erlaubt es, auf Cookies oder Logins zu verzichten. Bei der Auswahl der Schutzmöglichkeiten wird empfohlen, sich auf dem Portal des jeweiligen Browseranbieters genau zu informieren und dann erst eigene Maßnahmen zu treffen.

12.13 Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat

Das Zeitalter der digitalen Gesellschaft geht auch nicht spurlos am Personalausweisgesetz vorbei. Im Jahr 2010 wurde der neue digitale Personalausweis eingeführt. Man sah neben der Speicherung von Fingerabdrücken und einer qualifizierten elektronischen Signatur zur rechtssicheren digitalen Unterschrift auch die Speicherung einer elektronischen Identifikationsmöglichkeit (eID-Funktion) vor. Letztere sollte dazu dienen, sich gegenüber Behörden und Unternehmen online eindeutig gegenüber deren Online-Diensten identifizieren zu können.

Bürger konnten bei Ausgabe des Personalausweises wählen, ob sie diese Identifikationsmöglichkeit (eID-Funktion) zukünftig nutzen möchten.

Der Bundestagsdrucksache 18/11279 vom 22. Februar 2017 zur Änderung des Personalausweisgesetzes konnte man aber nun entnehmen, dass die Nutzung und die Verbreitung der eID-Funktion bisher hinter den Erwartungen zurückblieben. Bei zwei Dritteln der rund 51 Millionen ausgegebenen Ausweise sei die eID-Funktion deaktiviert.

Aber es gibt auch kaum Anwendungen diesbezüglich. Datenschützer warnten zudem auch permanent davor, die eID-Funktion zu nutzen, wenn nicht sichergestellt ist, dass heimlich das Passwort der eID-Funktion ausgelesen werden kann, z. B. durch Schadsoftware, welche die Tastatur-Eingabe am Rechner mit ausliest.

Nur die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Lesegeräte mit einer eigenen Tastatureingabe können dem derzeit Rechnung tragen. Alle anderen vom BSI zugelassenen Geräte sind aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nicht empfehlenswert. Möchte der Bund ein sicheres Verfahren anbieten, so muss auch aus datenschutzrechtlicher Sicht die Sicherheit des kompletten Verfahrens sichergestellt werden. Dem ist weiterhin nicht so. Die

Verantwortung auf den Bürger zu delegieren, ist nicht mehr zeitgemäß, zudem erfolgen immer mehr Hackerangriffe auf IT-Systeme. Zukünftige repräsentative Verfahren wie z. B. Online-Abstimmungen, Wahlen etc. wären mit Lesegeräten ohne eigene Tastatureingabe wie oben beschrieben von vornherein anfällig oder manipulierbar.

Da nur wenige Bürger die eID-Funktion bei Antragstellung des Personalausweises freigeschaltet haben wollten, entschloss sich der Gesetzgeber, nun das Personalausweisgesetz (PAuswG) dahingehend zu ändern, dass zukünftig die eID-Funktion für alle zukünftigen Personalausweise von vornherein freigeschaltet wird.

Zudem regelte man gleichzeitig in § 25 PAuswG, dass unter bestimmten Voraussetzungen zukünftig bestimmte Behörden im automatisierten Verfahren das Lichtbild aus dem Personalausweisregister abrufen können.

Dies konnten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder nicht unkommentiert lassen und positionierten sich in ihrer Entschließung bereits im Januar 2017 dahingehend, dass weiterhin die eID-Funktion freiwillig sein muss und die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste abgelehnt wird (siehe Anlage 3).

Die neuen Regelungen sind im Bundesgesetzblatt Nr. 46 vom 14. Juli 2017 veröffentlicht.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder fordern, dass weiterhin die Funktion der elektronischen Identifizierung mittels digitalem Personalausweis freiwillig bleibt. Zudem lehnen sie die vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste ab.

12.14 WannaCry

Im Frühjahr 2017 wurden weltweit zehntausende Computer Opfer eines Hackerangriffs durch die Schadsoftware WannaCry. Diese Software verschlüsselt die Daten auf den jeweils gehackten Compu-

tern und zeigt dann auf dem Bildschirm des Benutzers eine Lösegeldforderung an. Das Verfahren ist nicht neu. Seit Jahren wird in diesem Zusammenhang auch davon abgeraten, auf solche Lösegeldforderungen einzugehen, denn eine Entschlüsselung der Daten nach der Zahlung ist ungewiss. Tritt ein solcher Fall jedoch auf, hilft nur eine Anzeige bei der Polizei gegen Unbekannt. Der Rechner sollte umgehend neu installiert werden, bestenfalls mit einem Sicherungs-Image neueren Datums.

Neu bei diesem Angriff war allerdings, dass er massenhaft in über hundert Ländern gleichzeitig erfolgte. Man spricht vom größten Hacker-Angriff in der Geschichte der Cyber-Angriffe. Auch in Deutschland waren Behörden, Unternehmen sowie Privatpersonen betroffen. So manche Zuganzeige bei der Deutschen Bahn zeigte beispielsweise anstelle der Fahrverbindungen eine Lösegeldforderung an.

Sicherheitslücken in Betriebssystemen oder Systemanwendungen wird es allerdings wohl immer geben. Diese Lücken werden von den Herstellern zum Teil durch sogenannte Sicherheits-Updates (auch „Patches“ genannt) geschlossen. Deswegen ist es als Nutzer wichtig, immer auf die Aktualität der auf dem eigenen Computer installierten Software zu achten. Im Fall von WannaCry waren nur Windows-Rechner älterer Versionen betroffen. Bei aktuellen Versionen der Microsoft-Betriebssysteme war zuvor schon die Sicherheitslücke durch den Hersteller geschlossen worden. Nachdem WannaCry weltweit einen so großen „Erfolg“ hatte, stellte Microsoft zusätzlich Sicherheits-Updates für ältere Betriebssysteme, deren Support-Zyklen beendet sind – das sind Windows XP, Windows 8 als Client-Betriebssysteme und Windows Server 2003 – bereit.

Hinsichtlich der Nutzung von Rechnern mit dem Betriebssystem Windows XP warnte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 11. Tätigkeitsbericht unter Punkt 16.5. Mit der Ankündigung von Microsoft, das Betriebssystem ab dem 8. April 2014 nicht mehr mit Sicherheits-Updates zu versorgen, sah der TLfDI eine Gefahr für die Datensicherheit und somit für den Datenschutz.

Um das Sicherheitsrisiko bei Sicherheitslücken in Betriebssystemen oder Systemanwendungen zu minimieren, sind die vom Hersteller bereitgestellten Sicherheits-Updates zeitnah zu installieren. Client-Betriebssysteme, die im erweiterten Support keine Sicherheits-

Updates mehr erhalten, sind daher durch neuere Client-Betriebssysteme zu ersetzen. Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.

12.15 Zerstören Sie die Cayla-Puppe – wenn das Spielzeug mit- hört

Am 16. Februar 2017 wurde von den Medien eine etwas merkwürdige Meldung verbreitet. Besitzer der Puppe Cayla sollten diese zerstören. Was war geschehen? Cayla ist eine Spielzeugpuppe und wurde von der in Hong Kong ansässigen Firma Genesis Toys hergestellt und durch die britische Spielzeugfirma Vivid Toy Group Limited“vertrieben. In der Puppe war ein Mikrofon verbaut, welches die Sprache aufnehmen konnte und diese Daten an ein über Bluetooth verbundenes Gerät (z. B. Smartphone oder Tablet) weiter-schickte, wenn auf diesem die passende Cayla-App installiert und aktiviert war. Diese App schickte dann die Daten zur Analyse an einen Server, damit dieser eine passende Antwort generieren konnte, welche die Puppe dann von sich gab.

Die Bundesnetzagentur stufte die Puppe als eine „versteckte sende-fähige Anlage“ nach § 90 Telekommunikationsgesetz (TKG) ein, welches solche „Anlagen“ verbietet. Grund war, dass der Puppe nicht anzusehen war, dass diese als Mikrofon dient. Damit ist nicht nur der Betrieb der Puppe, also deren Benutzung, sondern sogar der Besitz einer solchen Puppe verboten. Daher auch die Meldung, dass Besitzer der Puppe diese umgehend zerstören sollen. Zudem sei die Bluetooth-Verbindung nicht abgesichert, was bedeutet, dass jeder in Reichweite der Puppe sich mit dieser verbinden konnte und diese als Abhöreinrichtung missbrauchen konnte. Nach Angaben der Stiftung Warentest (Ausgabe 09/2017, Seite 35 ff.) ist diese Eigenschaft der unsicheren Verbindung nicht selten anzutreffen. Der Teddy Toy-Fi oder der ebenfalls von Genesis Toys hergestellte Roboter i-Que besitzt ebenso diese Schwachstelle. Auch diese Spielzeuge bieten Apps zum „Abhören“ der Kinder und können auch mit Sprachnachrichten rückantworten. Einziger Unterschied ist hier, dass die Bun-desnetzagentur diese Spielzeuge noch nicht verboten hat.

Abgesehen von der potenziellen Abhörgefahr durch Personen, die sich in Funkreichweite dieser Spielzeuge befinden, ist auch gesell-

schaftlich ein Trend zu erkennen, dass immer mehr intelligente sprachgesteuerte Assistenten im Wohnbereich eingesetzt werden. Was mit „Siri“ auf dem iPhone begann und mit „Hello Google“ auch bei Android-Smartphones heute Stand der Technik ist, kommt nun in Form von Lautsprechern (Amazons „Alexa“, Googles „Home“ Lautsprecher, Apples „HomePod“) in die Wohnzimmer der Bevölkerung. Diese Geräte sind nicht so einfach zu kapern, wie dies bei den Spielzeugen der Fall ist, und von „verstecken sendefähige Anlagen“ kann auch keine Rede sein. Aber letztere Geräte reagieren auf Kommandoworte und schicken auch dann aufgenommene Sprache über das Internet an Server, welche die Kommandos interpretieren bzw. noch unbekannte Datenverarbeitungen damit vollziehen (so gibt es Forschungsarbeiten, die das Geschlecht, die Stimmung bzw. eine Personenidentifikation mit Sprachaufzeichnungen einschätzen können). Der Trend geht also ganz klar zur Vernetzung der Alltagsgegenstände. Über die Konsequenzen und was man eigentlich über sich dabei preisgibt, herrscht meist beim Nutzer Unklarheit. Im Fall der Puppe Cayla wurde ein Verbot ausgesprochen – allerdings nur aufgrund des „Versteckens“ der Funktion. Zahlreiche andere Produkte sind bereits im Alltag der Menschen angekommen. Hier sollte ein Bewusstsein in der Bevölkerung entstehen, bis wohin solche Geräte in das eigene Leben und das eigene Heim vordringen dürfen und aus welchen privaten Bereichen diese Art von Technik fernbleiben sollte. Im Kinderzimmer hat so etwas nach Auffassung des TLfDI jedenfalls nichts zu suchen.

Der TLfDI rät, „intelligente“ Spielzeuge ohne eine vorherige tiefgründige Recherche und Erklärung gegenüber dem Kind nicht einzusetzen. Sind die Verarbeitungsvorgänge unklar, rät der TLfDI von der Benutzung ganz ab. Das gleiche sollte der mündige Bürger beispielsweise auch für smarte Lautsprecher – ein neuer Techniktrend – beachten.

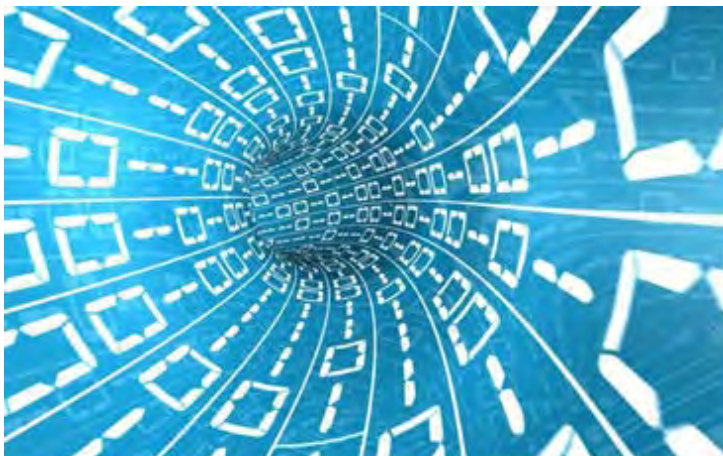


© fotomek – Runder Tisch / Fotolia.com

13 Veranstaltungen

13.1 Profiling

PROFILING
Big Data – Small Privacy
Zum Niedergang der Privatsphäre



© Dreaming Andy - Digital flow- fotolia.com

14. Februar 2017

10 Uhr

Augustinerkloster

Erfurt

Das Abfischen von Daten zur Bildung von Persönlichkeitsprofilen zum Beispiel beim Einkaufen, in sozialen Netzwerken, in persönlichen Blogs oder von Kontakt- und Bewegungsdaten ist heutzutage gang und gäbe. Oft geschieht es heimlich.

Aber warum? Wer hat Interesse an den Daten? Zu welchem Zweck werden die Daten genutzt? An wen werden sie weitergegeben?

Wir haben im Nachgang an unsere Profiling-Veranstaltung die von den Referenten freigegebenen Präsentationen als Reader für Sie zusammengefasst. Lassen Sie sich beim Nachlesen nochmals in die Untiefen des Daten-Meeres führen.

Reader zu Tagung zum Nachlesen unter
https://www.tlfdi.de/mam/tlfdi/veranstaltungen/reader_querformat_1_4_februar_2017.pdf

Erstellt aus den Vorträgen von:

Kai Biermann: Journalist bei Zeit Online, Teil des Zeit Online-Teams Investigativ/Daten. Er ist für die Bereiche Internet, Netzpolitik und Datenschutz zuständig.

Prof. Dr. Dorina Gumm: Professorin an der Fachhochschule Lübeck. Sie lehrt u. a. zu den Themen Web Information Systems, IT-Sicherheit sowie digitalisierte Gesellschaft. Im Projekt „Chaos macht Schule“ des CCC engagiert sie sich für Medienkompetenz und Technikverständnis bei Schülern.

Steffen Holly: Er ist Geschäftsfeldleiter Media Management & Delivery am Fraunhofer-Institut für Digitale Medientechnologie IDMT in Ilmenau.

Mike Kuketz: Gründer von Kuketz IT-Security. Er beschäftigt sich seit vielen Jahren intensiv mit den neuesten Entwicklungen im Bereich IT-Sicherheit und Datenschutz. Er ist derzeit u. a. auch Lehrbeauftragter an der Hochschule Karlsruhe und als Referent beim Landesmedienzentrum Baden-Württemberg tätig.

Prof. Dr. Kai-Uwe Sattler: Dekan der Fakultät für Informatik und Automatisierung. Er ist Leiter des Fachgebietes Datenbanken und Informationssysteme an der Technischen Universität Ilmenau.

13.2 Zusammenarbeit mit dem ERFA-Kreis Thüringen

ERFA-Kreise oder ausgeschriebene Erfahrungskreise werden in vielen Bereichen gegründet. Einer davon ist auch der Bereich des Datenschutzes und dort genauer der Bereich der behördlichen und betrieblichen Datenschutzbeauftragten .

Nach § 4f Abs. 1 Bundesdatenschutzgesetz (BDSG) sind bestimmte Unternehmen von Gesetzes wegen gezwungen, einen solchen Datenschutzbeauftragten zu benennen. Etwa dann, wenn besonders viele Personen (mehr als neun) mit der automatisierten (Computer) Verarbeitung von Daten beschäftigt sind oder wenn das Unternehmen in einer besonders benannten Sparte (z. B.: Meinungsforschung) tätig ist.

Dieser zu bestellende Beauftragte bedarf einer entsprechenden Qualifikation (Fachkunde und Zuverlässigkeit) und ist dem Leiter (Behörde) oder der Leitung (Unternehmen) unmittelbar zu unterstellen, wobei er allerdings weisungsfrei zu sein hat.

Dieser Datenschutzbeauftragte hat die Aufgabe, auf die Einhaltung der Vorschriften über den Datenschutz im Unternehmen oder der Behörde, in der er tätig ist, hinzuwirken und stellt damit – dies hat auch die Erfahrung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ergeben – ein wichtiges

Instrument zur Verwirklichung datenschutzrechtlicher Vorschriften dar.

Daher engagiert sich der TLfDI ebenfalls im ERFA-Kreis der Thüringer betrieblichen und behördlichen Datenschutzbeauftragten. Regelmäßig wird er zu deren Sitzungen eingeladen, informiert über die neusten Entwicklungen im Bereich Datenschutz und stellt sich den verschiedensten Fachfragen. Auch in diesem Berichtszeitraum sind Teilnahmen erfolgt. Regelmäßig wurde dabei das große Datenschutzthema, die Datenschutz-Grundverordnung, die Ende Mai 2018 Geltung erlangt, behandelt.

14 Vorträge – der TLfDI ist unterwegs!

Ob Datenschutz in Unternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden oder in medizinischen Einrichtungen, ob Videoüberwachung, Vorratsdatenspeicherung oder die Frage nach dem Umgang mit sozialen Netzwerken – datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Die von den Medien immer wieder aufgegriffenen Datenschutzskandale in Wirtschaftsunternehmen zeigen deutlich, dass der Datenschutz im privaten Bereich immer mehr in den Fokus des öffentlichen Interesses gerückt ist. Jeder Einzelne, ob als Kunde oder Arbeitnehmer, achtet mehr denn je auf einen verantwortungsvollen Umgang mit seinen Daten bei privaten Stellen. Umso wichtiger ist es für den TLfDI, dass sich auf der einen Seite die Stellen, die mit personenbezogenen Daten arbeiten, und auf der anderen Seite die Personen, um deren Daten es geht, gut beraten und betreut fühlen. Täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herein, ob der TLfDI nicht mit einem „Rundum-sorglos-Paket“ für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung durch seine Vorträge unterstützen kann. Der TLfDI selbst und seine Mitarbeiter haben im Berichtszeitraum abermals an mehr als 50 (!) Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im nicht-öffentlichen Bereich finden Sie auf den nächsten Seiten.

Intelligente Netze und Mess-Systeme

Smart Metering als Baustein für Energiewende und Energieeffizienz ?

FSU Jena

21. Januar 2016



Inhalt:

Rechtliche Rahmenbedingungen in Deutschland
Strommarkt 2.0

Daten-Selbstschutz

Veranstaltung FH Erfurt – Medienscout

27. Januar 2016



Inhalt:

Rechtliche Grundlagen
Bedrohungen des Grundrechts der informationellen Selbstbestimmung
Privatsphäre – Warum?
Selbstschutz
Schutz des Grundrechts
Digitale Selbstverteidigung – Broschüre mit Hinweisen zum Selbstdaten-
schutz

"Daten-Selbstschutz"

2. Datenschutztag Karl-Volkmar-Stoy-Schule Jena

2. März 2016



Inhalt:

Rechtliche Grundlagen
Bedrohungen des Grundrechts der informationellen Selbstbestimmung
Privatsphäre – Warum?
Selbstschutz
Schutz des Grundrechts
Digitale Selbstverteidigung – Broschüre mit Hinweisen zum Selbstdaten-schutz

2. Digitalisierungskonferenz EU-DSGVO

25. August 2016



Inhalt:

Europarechtliche Vorgaben

Ein wenig Dogmatik am Anfang – Typologie der Öffnungsklauseln

Sechs Beispiele für Öffnungsklauseln der DSGVO

Weitere Regelungsbedarfe aufgrund der DSGVO

„Beratungsaufgabe und Sanktionsrisiko“

Referatsleiter Referat 4
Johannes Matzke

Thüringer Zentrum für Existenzgründungen und Unternehmertum
(ThEx)

29. September 2016



Inhalt:

- Europäische Datenschutzgrundverordnung (EU-DSGVO)
- Unterschiede der DSGVO im Vergleich zum Bundesdatenschutzgesetz (BDSG) für Unternehmen
 - Betrieblicher Datenschutzbeauftragter (bDSB)
 - Auftragsdatenverarbeitung und DSGVO
 - Befugnisse und Sanktionsmöglichkeiten der Aufsichtsbehörde
- Ausblick
 - Gesetzgebungsverfahren Bund zum BDSG und Thüringen zum Thüringer Datenschutzgesetz (ThürDSG)

Informations- und Datenschutz
-gesetzliche Pflicht und
unternehmerische Verantwortung-
Datenschutz aktuell!

Wirtschaftsschutz - Forum Thüringen 2016

29. November 2016



Inhalt:

Historischer Hintergrund
IT-Sicherheit vs. Datenschutz: Gemeinsamkeiten und Unterschiede
Was ist das "Internet"?
Gefahren / Angriffsmethoden im Internet
Wie kann ich vorsorgen?

Datenschutz im Krankenhaus

Vortrag im Helios Klinikum Gotha
12. April 2017



Inhalt:

Der TLfDI!

Was ist Datenschutz?

Datenschutz in der Medizin – wichtig, weil:

Datenschutzrecht:

Gesetzliche Pflicht – Was sind die Vorgaben?

Abgrenzung zur Schweigepflichtentbindung

Thüringer Krankenhausgesetz

Technische und organisatorische Maßnahmen, § 9 BDSG

Datenschutz- Grundverordnung (DS-GVO)

Was ändert sich?

Safe-Harbor, die EuGH-Entscheidung vom 06.10.2015 und

Privacy-Shield – was ist da los?

26. April 2017



Inhalt:

Einführung – Datenübermittlung in die USA
Die Safe-Harbor-Entscheidung der EU-Kommission
Standardvertragsklauseln und Binding-Corporate-Rules als Alternativen zu Safe-Harbor
Die Enthüllungen Edward Snowdens und die Folgen
Die EuGH-Entscheidung vom 06.10.2015
Privacy-Shield – alter Wein in neuen Schläuchen?
Ausblick

Datenschutz in der Apotheke
– ein Auszug –

Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Apothekertag 2017, Erfurt,
10. Juni 2017



Inhalt:

Datenschutz – Die Aufsicht
Datenschutz – Das Juristische
Datenschutz – Die Problemfelder

„DS-GVO – Neuland?“

GSE Gruppe, MSECD – Datenschutzveranstaltung – Tabarz

20. September 2017

**Inhalt:**

Einführung – die DS-GVO
Profiling nach Art. 22 DS-GVO
Profiling mit Algorithmen – connected cars
Sensibilisierung von Betroffenen

Datenschutz und Fahrzeug?
Sie fahren gerade Ihrer Privatsphäre davon!

Tagung Autorecht Uni Bielefeld

5. Oktober 2017



Inhalt:

Informationsflüsse im Auto
Rechtsgrundlagen des Datenschutzes
Rechtliche Problemfelder und die Sicht des Datenschutzes

Die Neuerungen der DS-GVO
Im Hinblick auf vereinsrelevante Themen

Fortbildungsveranstaltung beim Landessportbund e. V. Erfurt

28. Oktober 2017



Die Neuerungen der DS-GVO

Im Hinblick auf vereinsrelevante Themen

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz und die
Informationsfreiheit (TLfDI)

28. Oktober 2017

Fortbildungsveranstaltung beim
Landessportbund e. V.

Inhalt:

Rechtsgrundlagen des Datenschutzes

Allgemeines zur DS-GVO

Rechtsnatur der DS-GVO

Definition personenbezogener Daten, Art. 4 DS-GVO

Grundsätze für die Verarbeitung Art. 5 DS-GVO

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Art. 6 DS-GVO

Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Art. 9 DS-GVO

Betroffenenrechte

Pflichten des Verantwortlichen

Effektive Durchsetzung

Fazit

Anlagen

Anlage 1

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich

(Düsseldorfer Kreis am 13./14. September 2016)

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-
Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Anlage 2

Entschließung

der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

**Wearables und Gesundheits-Apps –
Sensible Gesundheitsdaten effektiv schützen!**

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können. Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwen-

digen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).

Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.

Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.

Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.

Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Anlage 3

Entschließung zwischen den Konferenzen 2016/2017

Novellierung des Personalausweisgesetzes – Änderungen müssen
bürger- und datenschutzfreundlich realisiert werden!
(Umlaufentschließung vom 24. Januar 2017)

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets - wie bislang - nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.
- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an

der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.
- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

Anlage 4

Pressemitteilung
vom 19. Mai 2016

Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!

Wie aus einer Pressemitteilung des Unabhängigen Datenschutzzentrums Saarland zu entnehmen ist, stellt ein Urteil des Verwaltungsgerichts Saarland vom 18. Mai 2016 fest, dass der Betrieb von Wildbeobachtungskameras grundsätzlich dem Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) unterfällt und das Erheben, Verarbeiten oder Nutzen der mit einer Wildkamera erstellten Aufnahmen eine automatisierte Verarbeitung darstellen, sofern hiervon personenbezogene Daten möglicherweise betroffen sind. Damit sind die Kameras gemäß § 4d Abs. 1 BDSG meldepflichtig (siehe auch: <https://www.tlfdi.de/tlfdi/themen/video/>).

Auch nicht-öffentliche Stellen in Thüringen, die eine solche Kamera einsetzen wollen, müssen dies zuvor dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, wenn sie keinen betrieblichen Datenschutzbeauftragten haben. Der Inhalt der erforderlichen Meldepflicht ergibt sich aus § 4e BDSG. Damit bestätigt das Verwaltungsgericht die vom TLfDI vertretene Position.

Nach Auffassung des TLfDI hat das Urteil auch eine weitreichende Bedeutung für den Einsatz von **allen übrigen Videoüberwachungsanlagen** durch private Stellen, die (teilweise) öffentlich zugängliche Räume beobachten. Auch diese Stellen sind gegenüber dem TLfDI meldepflichtig.

Anlage 5

Pressemitteilung
vom 19. September 2017**Meldepflicht für (Wild-)Kameras bestätigt!**

Bereits mit Urteil vom 18. Mai 2016 stellte das Verwaltungsgericht Saarland fest, dass die Videoüberwachung mittels Wildbeobachtungskameras durch nicht-öffentliche Stellen (**u. a. natürliche und juristische Personen des Privatrechts**) grundsätzlich der Meldepflicht des § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) unterfällt. Die gegen das Urteil eingelegte Berufung von drei Jägern wurde mit Urteil vom 14. September 2017 durch das **Oberverwaltungsgericht Saarland** abgewiesen und die **Meldepflicht für Wildtierkameras bestätigt**. Die Revision gegen das Urteil wurde nicht zugelassen.

Auch der TLfDI vertritt, wie schon seit seiner Pressemitteilung vom 19. Mai 2016, die Auffassung, dass Wildtierkameras der Meldepflicht unterfallen.

Was allerdings für Wildkameras gilt, muss für alle anderen Kameras erst recht gelten:

Nicht-Öffentliche Stellen in Thüringen müssen Kameras vor dem Einsatz dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, sofern sie keinen betrieblichen Datenschutzbeauftragten bestellt haben. Der Inhalt der Meldung ergibt sich aus § 4e BDSG. Der TLfDI stellt auf seiner Website entsprechende Meldeformulare zur Verfügung:

(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v_.pdf).

„Bürgerinnen und Bürger sowie Unternehmen sollten dieser bußgeldbewehrten Meldepflicht rechtsbewusst nachkommen – für Fragen /Informationen stehe ich natürlich jederzeit zur Verfügung!“ – so Dr. Lutz Hasse.

Anlage 6

Pressemitteilung
vom 24. November 2017

**Microsoft trifft TLfDI
-Wirtschaft und Datenschutzaufsicht – geht das zusammen?-**

Der TLfDI, Dr. Lutz Hasse, ist Bundesvorsitzender des Arbeitskreises Datenschutz und Bildung aller Landesdatenschutzbeauftragten. In diesem Kreis werden derzeit bundesweite Lösungen etwa für Fragen erarbeitet, die sich im Zusammenhang mit Medienkompetenz von Lehrern und Schülern, aber auch mit Lernplattformen und digitalen „Schul-Büchern“ aufdrängen. Einer der großen Akteure in diesem Segment ist Microsoft, z. B. als bedeutender Cloud-Anbieter. In einem von der Wirtschaft und Politik aufmerksam beobachteten Prozess gehen der Global Player und die Datenschutzaufsichtsbehörden in Erfurt aufeinander zu, um gemeinsam datenschutzkonforme Lösungen zu finden.

Dr. Lutz Hasse: „Wir praktizieren ein neues Modell des Umgangs. Wir agieren nicht als Gegenspieler, sondern richten gemeinsam Wirtschaftsinteressen am Datenschutzrecht aus. Ohne gegenseitiges Vertrauen ist das nicht möglich – Microsoft ist hier zukunftsweisende Schritte gegangen, die Nachahmung finden sollten. Win-win für alle Beteiligten!“

Anlage 7

Pressemitteilung
vom 27. November 2017

Immelborn – AdActa

Seit kurzem liegt er vor: der **Zwischenbericht** des Untersuchungsausschusses 6/2 „Aktenlager Immelborn“ (Drucksache 6/4641). Beim Versuch, den Wertungsteil des Zwischenberichts zu verhindern, scheiterte die CDU-Fraktion vor dem Thüringer Verfassungsgerichtshof. Die Hauptfrage der Untersuchung lautete, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das damalige Thüringer Innenministerium (TIM) auf Amtshilfe zur Beräumung des Aktendepots verklagt habe, um dem damaligen Innenminister Geibert zu schaden. Das **Fazit** des **Zwischenberichtes** lautet: „Der dem Auftrag des Untersuchungsausschusses zugrunde liegende **Verdacht**, der TLfDI habe die Klage erhoben, um im damals anstehenden Wahlkampf dem politischen Konkurrenten in Gestalt des von ihm geführten TIM schaden zu wollen, konnte durch die die bisherige Beweisaufnahme **nicht erhärtet** werden.“

Ferner förderte der Zwischenbericht auch **andere wichtige Tatsachen und Feststellungen** ans Licht:

1. Die Zustellung der Bescheide des TLfDI durch **öffentliche Bekanntmachung** war **rechtmäßig** und erfolgte an den **richtigen Adressaten**.
2. Die getroffenen Maßnahmen des TLfDI waren **verhältnismäßig**.
3. Die **Ersatzvornahme** durch den TLfDI wird von der **Fachliteratur gestützt**.
4. Die **Polizei wollte** dem TLfDI **helfen**, wurde durch **Einwirkung der Hausleitung des TIM indes daran gehindert**.
5. Die Hausleitung des TIM **ließ gezielt Ablehnungsgründe gegen das Amtshilfegesuch generieren**, etwa: statt der vom TLfDI geforderten 10 Mann für 10 Tage, ließ die Hausleitung des TIM bei der Polizei anfragen, ob denn **100 Mann für 30 Tage** leistbar wären, **um dort eine ablehnende Haltung hervorzurufen**.
6. Das **TIM verweigerte dem TLfDI einen konstruktiven Dialog** völlig.
7. Das **Amtshilfeersuchen des TLfDI war zulässig und begründet**.

8. Der TLfDI durfte **nicht auf Private verwiesen** werden und die **Erfüllung polizeilicher Aufgaben** wäre durch die Amtshilfe **nicht gefährdet** gewesen.

9. Die **Bestellung des Nachtragsliquidators** erfolgte **zügig und rechtskonform**.

10. Für die **Beräumung des Aktenlagers** entstanden dem **Freistaat keine Kosten**.

Anlage 8

Kurzpapier Nr. 1**Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO**

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Altes Recht = neues Recht?

Das aus dem BDSG bekannte Verzeichnissverzeichnis (§ 4g Abs. 2 und 2a BDSG; dort „Übersicht“ genannt) wird mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und – neu – auch jeder Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet. Es wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verzeichnissverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein.

Stellen mit weniger als 250 Mitarbeitern

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen (z. B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder

- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist. Da es anders als in Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) nicht darauf ankommt, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt, sondern jedes Risiko für die Rechte und Freiheiten bezüglich der Verarbeitung zu betrachten ist, wird vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten sein.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Anders als im bisherigen BDSG ist eine Möglichkeit für jedermann, in das Verzeichnis von Verarbeitungstätigkeiten Einsicht zu nehmen, nach der DS-GVO nicht vorgesehen. Ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Meldepflichten von manchen Unternehmen an die Aufsichtsbehörde. Erstellt und vorgehalten werden müssen die Verzeichnisse dennoch, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung zu stellen sind (siehe Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Inhalt des Verzeichnisses für Verantwortliche (Art. 30 Abs. 1 DS-GVO)

Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DS-GVO wesentliche Angaben zur Verarbeitung beinhalten wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger. Verantwortliche Stellen, die bereits jetzt über ein strukturiertes Verzeichnissesverzeichnis oder eine strukturierte Datenschutzdokumentation zu den Verfahren verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine Probleme haben.

Inhalt des Verzeichnisses für Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

Ein Verzeichnis beim Auftragsverarbeiter zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätig-

keiten der Verarbeitung war vom BDSG bislang nicht vorgeschrieben. Nach Art. 30 Abs. 2 DS-GVO ist ein solches Verzeichnis jedoch künftig zu erstellen. Auch hier sind die Pflichtangaben überschaubar, so dass der Aufwand, dieses Verzeichnis zu erstellen, als eher gering einzustufen sein wird.

Beschreibung technischer und organisatorischer Maßnahmen

Art. 30 Abs. 1 lit. g und Art. 30 Abs. 2 lit. d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

Rechtsfolgen bei Verstoß

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße sanktioniert werden.

Das Verzeichnis als Teil der Rechenschaftspflicht

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden.

Ausblick: Wesentliche Rolle des Verzeichnisses und Muster-Vorlage der Datenschutzaufsichtsbehörden

Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verfahrensverzeichnisse eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmä-

ge Verarbeitung personenbezogener Daten sicherstellen zu können. Die deutschen Aufsichtsbehörden werden im Jahr 2017 eine Muster-Vorlage sowie weitere Hinweise für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO bereitstellen.

Unsere Empfehlung

Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Übergangszeit bis zur Geltung der DS-GVO am 25. Mai 2018 sollte dazu genutzt werden, die bereits bestehende Verfahrensdokumentation an die neu-en Anforderungen anzupassen.

Anlage 9

Kurzpapier Nr. 2
Aufsichtsbefugnisse/Sanktionen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs- und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Neben diesen verwaltungsrechtlichen Maßnahmen können Verstöße auch mit hohen Geldbußen sanktioniert werden.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsvfahren (Art. 58 -GVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grundverordnung darstellen, bzw. Verwarnungen, wenn mit Datenverarbeitungen bereits gegen die Grundverordnung verstoßen wurde. Darüber hinaus können Verantwortliche und Auftragsverarbeiter künftig im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist künftig auch die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation möglich. Die Befugnis der Aufsichtsbehörden, Beschränkungen und Verbote von Datenverarbeitungen und die Berichtigung oder Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anzuordnen, bleibt unbe-

rührt. Nicht zuletzt können mit Inkrafttreten der Grundverordnung Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen. Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Zu beachten ist, dass sich die genannten behördlichen Maßnahmen zukünftig nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter richten können. Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei den Verantwortlichen und auch Auftragsverarbeiter Mitwirkungspflichten treffen. Insbesondere können die Aufsichtsbehörden den Verantwortlichen und Auftragsverarbeiter sowie deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind. Alle Anordnungen können mit Zwangsmitteln, wie Zwangsgeldern, durchgesetzt werden. Rechtsschutz bei Zweifeln an der Rechtmäßigkeit der Anordnungen der Aufsichtsbehörde ist wie bisher auch im verwaltungsgerichtlichen Verfahren gewahrt.

Verhängung von Geldbußen (Art. 83 DS-GVO)

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Der Rahmen für die Geldbußen wird mit der DS-GVO deutlich erhöht. Dies trägt der gestiegenen Bedeutung des Datenschutzes Rechnung. So können Geldbußen von bis zu 10.000.000 € bzw. bei Unternehmen bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden (z. B. ist eine weitere erwähnenswerte Neuerung gegenüber der aktuellen Rechtslage, dass unter dem Regime der DS-GVO auch ein Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten mit einer Geldbuße geahndet werden kann). Bei bestimmten, besonders schwerwiegenden Verstößen, darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage, sind Geldbußen von bis zu 20.000.000 € möglich. Gegen Unternehmen kann diese Grenze sogar noch überschritten werden, nämlich bis zu 4% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Für den Fall der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO ist ebenfalls die Verhängung einer Geldbuße von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen. In allen drei Fallgestaltungen richtet sich die maximale Obergrenze für die Geldbuße danach, welcher der Beträge höher ist.

Hierbei geht die DS-GVO von einem gegenüber Art. 4 Nr. 18 DS-GVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem Bußgeldverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DS-GVO zu entnehmen. Danach gilt der aus dem Kartellrecht entlehnte weite, funktionale Unternehmensbegriff nach Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dies hat zur Folge, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde gelegt wird. Nach dem Wortlaut der DS-GVO reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch ein für das Unternehmen agierender externer Beauftragter gehandelt hat. Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt. Für die Zumessung der Geldbußen gilt zuvörderst der Grundsatz, dass die Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Art. 83 Abs. 2 S. 2 DS-GVO enthält eine Auflistung von Kriterien, die bei der Entscheidung über die Verhängung und die Höhe einer Geldbuße (ggf. auch einem Absehen davon, vgl. ErwGr. 148) gebührend im Einzelfall berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist künftig auch die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere, ob und wie die Verantwortlichen mit den Aufsichtsbehörden zusammen gearbeitet haben, um Verstößen abzuhelpen und ihre möglichen nachteiligen Auswirkungen zu mindern, und ob sie die Verstöße eigenständig mitgeteilt haben. Ferner ist auch der Grad der Verantwortung des Verantwortlichen bzw. Auftragsverarbeiters unter Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maß-

nahmen ein zu berücksichtigendes Kriterium. Mithin wird im Einzelfall zu überprüfen sein, inwieweit ein Unternehmen im Rahmen seiner internen Organisation, etwa durch Ausgestaltung seiner Strukturen, Arbeitsprozesse und Kontrollmechanismen, Vorkehrungen getroffen hat, die dazu dienen, die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen, bzw. inwieweit die interne Organisation diesbezüglich Mängel aufweist. Zudem können jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, Berücksichtigung finden. Abzuwarten bleibt, in welcher Form der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 lit. k DS-GVO umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO zu erlassen.

Anlage 10

Kurzpapier Nr. 3**Verarbeitung personenbezogener Daten für Werbung**

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Keine Detailregelung für Werbung

Mit der DS-GVO fallen alle detaillierten Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für werbliche Zwecke weg.

Werbung nach Interessenabwägung

Grundlage für die Beurteilung der Zulässigkeit von Werbung ist in Zukunft, abgesehen von einer Einwilligung, eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Ausgangspunkt für die zu treffende Abwägungsentscheidung ist Erwägungsgrund (ErwGr.) 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ Ferner gibt ErwGr. 47 DS-GVO im Rahmen der durchzuführenden Interessenabwägung vor, die „vernünftigen Erwartungen der betroffenen Person“, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen. Wann diese Voraussetzungen vorliegen, ist derzeit noch nicht abschließend geklärt. Dem Working Paper der Art. 29 Datenschutzgruppe (WP 217, S. 51), das sich allerdings auf die Datenschutzrichtlinie 95/46/EG bezieht, können insoweit erste Interpretationshinweise entnommen werden. Die vernünftigen Erwartungen der betroffenen Person werden bei Maßnahmen zur werblichen Ansprache maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt werden. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene werbliche Nutzung der Daten,

geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Insoweit ist im Rahmen der Interessenabwägung zu berücksichtigen, dass die von Werbung betroffenen Personen ein jederzeitiges und umfassendes Widerspruchsrecht haben (Art. 21 Abs. 2 DS-GVO), auf das sie ausdrücklich hinzuweisen sind (Art. 21 Abs. 4 DS-GVO). Der Werbewiderspruch hat nach Art. 21 Abs. 3 DS-GVO zur Folge, dass personenbezogene Daten für Werbezwecke nicht mehr verarbeitet, insbes. verwendet werden dürfen. Im Übrigen ist zu berücksichtigen, ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt (ErwGr. 47 DS-GVO). Ferner sind bei der Interessenabwägung auch die allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO zu berücksichtigen, also insbesondere:

- faire Verfahrensweise
- dem Verarbeitungszweck angemessen
- in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten)

Diese Grundsätze sprechen jedenfalls dagegen, Profile zur werblichen Ansprache (Werbescores) zu erstellen, die z. B. Informationen aus sozialen Netzwerken berücksichtigen. Eingriffsintensivere Maßnahmen wie Profilbildung sprechen eher dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. Unabhängig von der Interessenabwägung müssen die Informationspflichten nach den Art. 13, 14 DS-GVO eingehalten werden.

Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Art. 9 DS-GVO enthält keine Erlaubnisnorm für die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Werbung. Dies ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person zulässig. Von Relevanz ist dies z. B. für Unternehmen und Berufe des Gesundheitswesens (Apotheken, Sanitätshäuser, Optiker, Orthopäden usw.).

Besondere Grenzen aus § 7 UWG

Auch nach neuem Recht wird die Interessenabwägung bei der Nutzung der Kontaktdaten von Verbrauchern für Telefon- und Faxwerbung dazu führen, dass diese weiterhin nur mit einer vorherigen ausdrücklichen Einwilligung erlaubt ist. Alles andere wäre im Hinblick auf die klaren Regelungen in § 7 des Gesetzes gegen den un-

lauteren Wettbewerb (UWG) mit den vernünftigen Erwartungen der Betroffenen (ErwGr. 47 DS-GVO) nicht zu vereinbaren. Ebenso ist eine Kontaktdatennutzung für E-Mail- und SMS-Werbung außerhalb einer Einwilligung nur im Fall der Eigenwerbung bei Bestandskunden unter den Maßgaben von § 7 Abs. 3 UWG zulässig. Im Übrigen bleibt abzuwarten, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen (z. B. ausschließliche Opt-in-Lösung) für werbliche Ansprachen enthalten wird.

Fortgeltung von Einwilligungen

Bisher erteilte Einwilligungen wirken nach Erwägungsgrund 171 der DS-GVO fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen. Die im Wirtschaftsleben EU-weit vorhandenen Einwilligungen sind auf ihre Wirksamkeit hin zu überprüfen. Dabei ist u. a. von Bedeutung, ob auf Grundlage der neuen Anforderungen nach Art. 7 Abs. 4 der DS-GVO eine freiwillige Erklärung abgegeben und dass die Altersgrenze für die Einwilligungsfähigkeit bei Inanspruchnahme von Diensten der Informationsgesellschaft nach Art. 8 Abs. 1 der DS-GVO berücksichtigt wurde.

„Koppelungsverbot“ bei Einwilligungen für Werbung

Das bisher schon bestehende Koppelungsverbot für Werbung findet sich auch in der DS-GVO wieder, ist aber nicht mehr davon abhängig, ob ein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO). Bei „kostenlosen“ Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen“ (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung“), muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung.

Ausblick für den künftigen Umgang mit personenbezogenen Daten für Werbung

Soweit Werbung nicht auf einer wirksamen Einwilligung der betroffenen Person beruht, wird für die Zulässigkeit von Werbung in Zukunft fast ausschließlich die nach Art. 6 Abs. 1 lit. f DS-GVO vorgeschriebene Interessenabwägung maßgeblich sein. Inwieweit es in Europa gelingen wird, die in Deutschland entwickelten Maßstäbe auch unter Geltung der DS-GVO aufrechtzuerhalten, wird sich zeigen. Anzustreben sind für diesen Bereich möglichst EU-weite Verhaltensregeln. Sollte das nicht für die wesentlichen Bereiche der Werbung gelingen, wird mit Leitlinien des Europäischen Datenschutzausschusses auch zu diesem Thema zu rechnen sein.

Anlage 11

Kurzpapier Nr. 4
Datenübermittlung in Drittländer

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen vor: Art. 44 – 49. Länder außerhalb der EU/des EWR werden in der DS-GVO als „Drittländer“ bezeichnet, in der Praxis wird auch der Begriff „Drittstaat“ verwendet. Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den in den Art. 45 ff. geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer auch alle übrigen Anforderungen der DS-GVO (z. B. Art. 9 Abs. 3) an die in Rede stehende Datenverarbeitung eingehalten werden (1 Stufe). Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Art. 44 zusätzlich die spezifischen Anforderungen der Art. 45 ff. an die Übermittlung in Drittländer beachtet werden (2. Stufe; „2-Stufen-Prüfung“). Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 2. HS (siehe auch Erwägungsgrund (ErwGr.) 101)). Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO)**
- **Vorliegen geeigneter Garantien (Art. 46 DS-GVO) oder**
- **Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO).**

1. Feststellung der Angemessenheit des Datenschutzniveaus im Drittstaat durch die Kommission (Art. 45 DS-GVO)

Die Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist. Eine Datenübermittlung auf Grundlage eines solchen Angemessenheitsbeschlusses bedarf keiner weiteren Genehmigung durch die für den Verantwortlichen oder Auftragsverarbeiter zuständige nationale Aufsichtsbehörde. Die DS-GVO sieht eine Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse vor (Art. 46 Abs. 5 S. 2). Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt (C(2016) 4176 final)).

2. Vorliegen geeigneter Garantien (Art. 46 DS-GVO)

Eine Datenübermittlung in ein Drittland ist weiter zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien zur Gewährleistung eines angemessenen Schutzniveaus vorgesehen hat. Folgende Garantien kommen in Betracht:

a) Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Art. 46 Abs. 2 lit. b, Art. 47)

Verbindliche interne Datenschutzvorschriften (BCR) wurden schon bisher in der Praxis verwendet und sind nun in der DS-GVO (anders als in der noch geltenden EU-Datenschutzrichtlinie 95/46/EG) ausdrücklich als Möglichkeit zur Erbringung „geeigneter Garantien“ für Datenübermittlungen in Drittländer geregelt. Sie können vor allem bei international tätigen Konzernen mit internem Datenfluss (auch) in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest. Die BCR müssen einen Schutz bieten, der im Wesentlichen der DS-GVO entspricht. Der Mindest-Inhalt ist in Art. 47 Abs. 2 festgelegt. Zudem müssen die BCR für alle betreffenden Mitglieder der Unternehmensgruppe rechtlich bindend sein und den betroffenen Personen durchsetzbare Rechte gewähren (Art. 47 Abs. 1

lit. a und b). Die Genehmigung der BCR erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1). Die konkreten Datenübermittlungen auf Grundlage der BCR werden dann nicht mehr einzeln genehmigt.

b) Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 lit. c und d)

Schließen der Datenexporteur und der Datenimporteur einen Vertrag unter Verwendung der Standarddatenschutzklauseln der Kommission, ist der darauf basierende Datentransfer ohne weitere Genehmigung durch die Aufsichtsbehörde zulässig (vorbehaltlich der weiteren Anforderungen nach der DS-GVO). Auch den Aufsichtsbehörden ist es möglich, eigene Standarddatenschutzklauseln zu entwerfen. Diese bedürfen der Abstimmung im Kohärenzverfahren und sind anschließend von der Kommission förmlich zu genehmigen.

Die bereits bestehenden EU-Standardvertragsklauseln gelten gemäß Art. 46 Abs. 5 S. 2 ausdrücklich fort. Sofern die Standarddatenschutzklauseln in unveränderter Form verwendet werden, sind die Datenübermittlungen genehmigungsfrei. Dies gilt auch noch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standarddatenschutzklauseln stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden (ErwGr. 109). Bei solchen Hinzufügungen sollten Unternehmen jedoch eine gewisse Vorsicht walten lassen, da im Falle eines inhaltlichen Widerspruchs zu den Standarddatenschutzklauseln die Übermittlung nicht mehr genehmigungsfrei ist.

c) Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. e und f)

Neu hinzugekommen ist die Möglichkeit, Datenübermittlungen auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Art. 40 zu legitimieren, sofern diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sind und von der zuständigen Aufsichtsbehörde genehmigt worden sind.

Auch Zertifizierungen nach Art. 42 können nun zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters als rechtliche Grundlage für einen Datentransfers in ein Drittland herangezogen werden, wenn die Zertifizierungsmechanismen zuvor genehmigt worden sind.

Die europäischen Aufsichtsbehörden werden in der Folgezeit die für eine praktische Anwendung dieser Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen erarbeiten.

d) Einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3)

Ebenso können einzeln ausgehandelte individuelle Vertragsklauseln eine Datenübermittlung in ein Drittland legitimieren, allerdings nur nach Genehmigung der Aufsichtsbehörde und Durchführung des Kohärenzverfahrens nach Art. 63.

e) Rechte der betroffenen Personen

Gemäß Art. 46 Abs. 1 a. E. ist es bei allen in Betracht kommenden geeigneten Garantien im Sinne von Art. 46 zusätzlich erforderlich, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe einzuräumen.

3. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Eine Datenübermittlung kann in einer Reihe besonderer, vom Gesetz explizit genannter und abschließender Fälle, auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen. Die hierfür von der DS-GVO definierten Ausnahmetatbestände sind gemäß ihrem Ausnahmecharakter eng auszulegen.

a) Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a)

Eine wirksame Einwilligung der betroffenen Person in die Datenübermittlung in ein Drittland setzt zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall voraus. Weiter ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären, d.h. insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte ggf. nicht durchgesetzt werden können. Auch ist die betroffene Person darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann (Art. 7 Abs. 3).

b) Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b und c)

Eine Datenübermittlung in ein Drittland ist (vorbehaltlich der weiteren Anforderungen der DS-GVO) zulässig, wenn und soweit die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist. Wesentlich ist hier

jeweils die strikte Erforderlichkeit gerade dieser Datenübermittlung zur Erfüllung des Vertragszwecks.

c) Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d)

Die Übermittlung kann auch zulässig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. In Betracht kommen nur wichtige öffentliche Interessen, die im Recht der Europäischen Union oder des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sind (Art. 49 Abs. 4). Wie aus Erwägungsgrund 112 hervorgeht, hatte der Gesetzgeber insoweit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit im Auge, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden.

d) Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e)

Auch die Verfolgung von Rechtsansprüchen kann eine Datenübermittlung legitimieren, wenn die Datenübermittlung hierzu erforderlich ist. In Erweiterung der bisherigen Regelung im BDSG kommt auch die Geltendmachung von Rechtsansprüchen in außergerichtlichen Verfahren in Betracht (ErwGr. 111).

e) Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 lit. f)

Ist die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage, ihre Einwilligung zu erteilen, darf die Datenübermittlung dennoch durchgeführt werden, soweit dies zum Schutz ihrer lebenswichtigen Interessen oder derjenigen anderer Personen erforderlich ist.

f) Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 UAbs. 2 S. 1)

Im Einzelfall kann eine Datenübermittlung in ein Drittland legitimiert sein, wenn ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung besteht, die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwiegenden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen und der Verantwortliche durch geeignete Garantien den Schutz personenbezogener Daten gewährleistet. Voraussetzung für diese Übermittlungserlaubnis ist ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung, dem eine herausgehobene und besondere Bedeutung zukommt. Zudem muss die Übermittlung unbedingt erforderlich

sein zur Verfolgung dieses berechtigten Interesses. Die Übermittlung darf sich nicht bereits auf einen der oben genannten Erlaubnistatbestände stützen lassen. Wird eine Übermittlung in ein Drittland auf Grundlage eines zwingenden berechtigten Interesses in einem absoluten Einzelfall durchgeführt, ist sowohl die Aufsichtsbehörde als auch die betroffene Person hierüber zu informieren (Art. 49 Abs. 1 UAbs. 2 S. 2 und 3).

Anlage 12

Kurzpapier Nr. 5**Datenschutz-Folgenabschätzung, Art. 35 DS-GVO**

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr. 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

Zeitpunkt der Durchführung einer DSFA

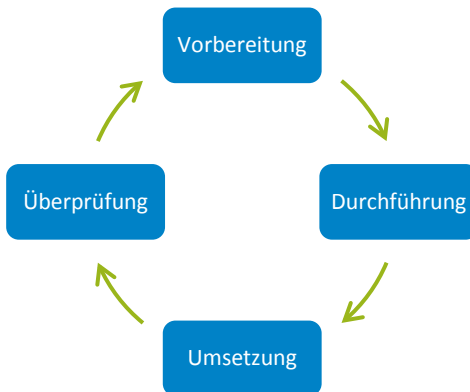
Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

Wie kann eine DSFA durchgeführt werden?

Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DS-GVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Methode wird dem Verantwortlichen mehr Spielraum gelassen. Werden be-

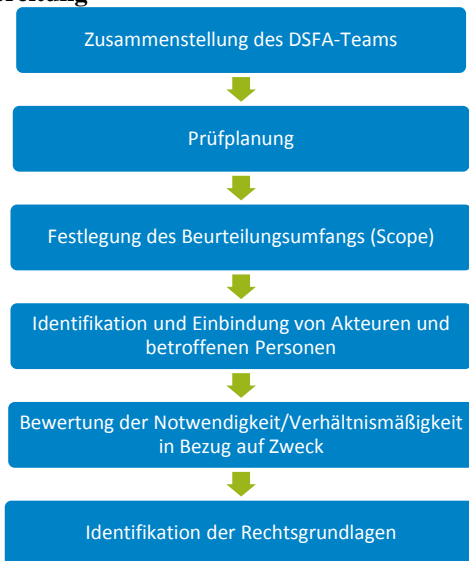
stehende Methoden oder Standards eingesetzt, ist zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu behandeln sind.

Eine DSFA ist kein einmaliger Vorgang. Sollten sich z.B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen:



Die Bestandteile der Hauptprozessschritte werden im Einzelnen nachfolgend dargestellt.

Vorbereitung



1. *Zusammenstellung des DSFA-Teams*

Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt. Der Datenschutzbeauftragte steht diesem während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, z. B. Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2. *Prüfplanung*

Da eine DSFA meist ein komplexer Prozess ist, der viele Mitwirkende einbindet, ist eine Prüfplanung (z. B. mit Methoden des Projektmanagements) empfehlenswert.

3. *Festlegung des Beurteilungsumfangs (Scope)*

Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

4. Identifikation und Einbindung von Akteuren und betroffenen Personen

Die Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht der Verantwortliche den Datenschutzbeauftragten zurate (Art. 35 Abs. 2 DS-GVO). Ggf. holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Art. 35 Abs. 9 DS-GVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, z. B. von Betriebsräten.

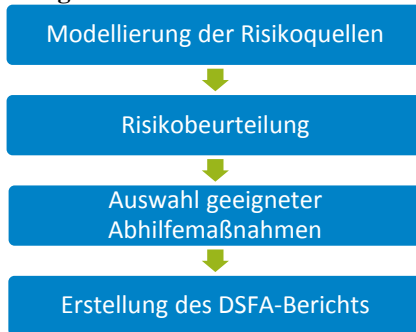
5. Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck

Die im vorigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der Betroffenen weniger stark eingreifen. Ggf. nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6. Identifikation der Rechtsgrundlagen

Aufbauend auf dem vorigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.

Durchführung



7. *Modellierung der Risikoquellen*

Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8. *Risikobeurteilung*

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen (ErwGr. 75 f.).

9. *Auswahl geeigneter Abhilfemaßnahmen*

Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

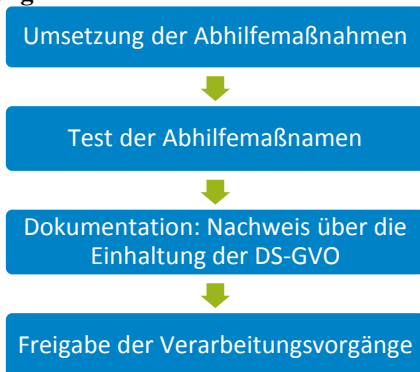
10. Erstellung des DSFA-Berichts

Der DSFA-Bericht enthält gem. Art. 35 Abs. 7 DS-GVO jedenfalls die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Weitere Schritte nach Durchführung der DSFA

Die folgenden Schritte dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkoppelung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.

Umsetzung



11. Umsetzung der Abhilfemaßnahmen

Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen

(insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DS-GVO genügen.

12. Test der Abhilfemaßnahmen

Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13. Dokumentation: Nachweis über die Einhaltung der DS-GVO

Gem. Art. 5 Abs. 2 DS-GVO hat der Verantwortliche eine umfassende Dokumentations- und Rechenschaftspflicht, durch die die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14. Freigabe der Verarbeitungsvorgänge

Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden.

Überprüfung

Ggf. Überprüfung und Audit der DSFA



Fortschreibung

15. Ggf. Überprüfung und Audit der DSFA

Um eine ordnungsgemäße Durchführung sicherzustellen, kann es sinnvoll sein, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Auch könnte der Datenschutzbeauftragte, der gemäß Art. 35 Abs. 2 DS-GVO sowieso einzubeziehen ist, die DSFA abschließend prüfen und das Ergebnis der Leitungsebene des Verantwortlichen mitteilen.

16. Fortschreibung

Die DSFA ist kein strikt linearer oder abgeschlossener Prozess. Vielmehr muss die Einhaltung der DS-GVO während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden. Hierfür bietet sich ein Datenschutz-Managementsystem an. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

Umgang mit hohen Restrisiken

Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

Fazit

Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem BDSG dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.

Anlage 13

Kurzpapier Nr. 6

Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auskunftsrecht als zentrales Recht zur Schaffung von Transparenz

Wie schon nach der bisherigen Rechtslage haben betroffene Personen das Recht mit formlosem Antrag und ohne Begründung von einem Verantwortlichen Auskunft über dort gespeicherte personenbezogene Daten zu verlangen. Die Auskünfte können es beispielsweise erleichtern, gezielt weitere Rechte, wie auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“), geltend zu machen.

Umfang des Auskunftsrechts

Nach Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu.

Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.

Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

Weiterhin sind bei der Datenauskunft vom Verantwortlichen nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden (mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
- geplante Speicherdauer falls möglich, andern-falls die Kriterien für die Festlegung der Speicherdauer,
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
- Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

Im Falle der Datenübermittlung in Drittländer ist über die insoweit gegebenen Garantien gemäß Art. 46 DS-GVO zu informieren (z. B. vereinbarte Standard-Datenschutzklauseln, verbindliche interne Datenschutzvorschriften, d. h. BCR). Keine Drittländer sind die EU-Mitgliedsstaaten

Form der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person kann nach Art. 12 Abs. 1 Sätze 2 und 3 DS-GVO je nach Sachverhalt schriftlich, elektronisch oder – auf Wunsch der betroffenen Person – mündlich erfolgen. Der Verantwortliche stellt eine Kopie der Daten zur Verfügung (Art. 15 Abs. 3 Satz 1 DS-GVO). Stellt die betroffene Person ihren Auskunftsantrag elektronisch, ist die Auskunft nach Art. 15 Abs. 3 Satz 2 DS-GVO in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. im PDF-Format). Als datenschutzfreundlichste Gestaltung wird in Erwägungsgrund (ErwGr.) 63 Satz 4 ein vom Verantwortlichen eingerichteter Fernzugriff der betroffenen

Person auf ihre eigenen Daten bezeichnet. Alle Kommunikationswege müssen angemessene Sicherheitsanforderungen erfüllen.

Frist für die Auskunftserteilung

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats; nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden, worüber die betroffene Person zu informieren ist (Art. 12 Abs. 3 Satz 3 DS-GVO). Der Verantwortliche muss (vorbereitend) geeignete organisatorische Maßnahmen treffen, damit die betroffene Person eine beantragte Auskunft zeitnah und in verständlicher Form erhalten kann (Art. 12 Abs. 1 Satz 1 und Art. 5 Abs. 2 DS-GVO).

Kosten der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person (z. B. als Kopie) muss durch den Verantwortlichen regelmäßig unentgeltlich erfolgen, Art. 12 Abs. 5 Satz 1 DS-GVO. Für weitere Kopien kann er ein angemessenes Entgelt fordern. Außerdem kann bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt für die Auskunft verlangt werden (Art. 12 Abs. 5 Satz 2, ErwGr. 63).

Identitätsprüfung

Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag).

Grenzen des Auskunftsrechts

Bei einer großen Menge von gespeicherten Informationen über die betroffene Person kann der Verantwortliche verlangen, dass präzisiert wird, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftersuchen konkret bezieht (ErwGr. 63 Satz 7). Das kann z. B. bei Banken oder Versicherungen mit umfangreichen Vertragsbeziehungen zu der betroffenen Person der Fall sein.

Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht

führen (Art. 12 Abs. 5 S. 2 DS-GVO). Die betroffene Person muss jedoch (und zwar kostenfrei) ihr Recht in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (ErwGr. 63). Eine Ablehnung oder Kostenerstattung kommt daher nur in Ausnahmefällen in Betracht. Der Verantwortliche trägt die Beweislast für das Vorliegen eines unbegründeten oder exzessiven Antrags (Art. 12 Abs. 5 Satz 3 DS-GVO). Er muss der betroffenen Person in der Regel die Gründe für die Verweigerung der Auskunft mitteilen und sie über Rechtsschutzmöglichkeiten informieren (Art. 12 Abs. 4 DS-GVO). Das BDSG-neu enthält in § 34 noch weitere Eingrenzungen des Auskunftsrechts, insbesondere für Archivdaten und Protokollierungsdaten.

Ob und wenn ja wie weit die Regelungen des BDSG-neu zur Einschränkung der Betroffenenrechte wegen des bestehenden Anwendungsvorrangs der DS-GVO angewendet werden können, bleibt eine Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Beachtung Rechte Dritter

Die Auskunftserteilung an die betroffene Person darf nach Art. 15 Abs. 4 DS-GVO sowie ErwGr. 63 Satz 5 die Rechte des Verantwortlichen oder anderer Personen nicht beeinträchtigen, was bei Geschäftsgeheimnissen oder bei Daten mit Bezug auch auf andere Personen der Fall sein kann. Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird.

Rechtsfolgen bei Verstoß

Unterlassene oder nicht vollständige Auskunftserteilungen an betroffene Personen sind nach Art. 83 Abs. 5 lit. b DS-GVO mit einer hohen Geldbuße bedroht.

Empfehlung

Es ist für Verantwortliche ratsam, rechtzeitig im eigenen Interesse organisatorische Vorkehrungen für zügige und korrekte Auskunftserteilungen zu treffen.

Anlage 14

Kurzpapier Nr. 7

Markortprinzip: Regelungen für außereuropäische Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Regelung des Markortprinzips in Art. 3 Abs. 2 DS-GVO

Das Markortprinzip schließt unter bestimmten Bedingungen auch Unternehmen, die nicht in der EU niedergelassen sind, in den Anwendungsbereich der DS-GVO ein.

Seit In-Kraft-Treten der EU-Datenschutzrichtlinie im Jahr 1995 haben sich neue Fragestellungen zum Anwendungsbereich des europäischen Datenschutzrechts entwickelt, beispielsweise mit Blick auf die fortschreitende Verlagerung von Geschäftsaktivitäten ins Internet (eCommerce). Sie erfordern keine physischen Betriebs- und Organisationsstrukturen in Europa, die als direkter Anknüpfungspunkt für die Anwendbarkeit europäischen Datenschutzrechts dienen könnten.

Der europäische Gesetzgeber erstreckt den Anwendungsbereich des europäischen Datenschutzrechts mit Einführung des Markortprinzips auf datenschutzrechtlich relevante Geschäftsaktivitäten von Unternehmen, die keine Niederlassungen in der EU besitzen und damit an sich außerhalb des territorialen Anwendungsbereichs nach Art. 3 Abs. 1 DS-GVO liegen würden. Unter den von Art. 3 Abs. 2 lit. a und lit. b DS-GVO festgelegten Bedingungen erstreckt sich der Anwendungsbereich der DSGVO auf Verarbeitungen personenbezogener Daten von Betroffenen, die sich in der EU befinden, ohne Rücksicht auf physische Organisations- oder Betriebsstrukturen von Unternehmen in der EU.

1. Anknüpfungspunkt: Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 lit. a DS-GVO)

Die DS-GVO findet Anwendung, wenn eine Daten-verarbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Waren oder Dienst-leistungen anzubieten. Das Unternehmen muss dies offensichtlich beabsichtigen (vgl. ErwGr. 23). Die Zahlung eines Entgeltes für das Waren- oder Dienstleistungsangebot ist hierbei für die Anwendbarkeit der DS-GVO irrelevant, sondern es sollen explizit auch unentgeltliche Angebote, z. B. Dienstleistungen durch soziale Netzwerke, darunter fallen.

Ein maßgeblicher Anknüpfungspunkt ist die Ausrichtung bestimmter Werbe- bzw. Verkaufsmaßnahmen auf Personen, die sich in der EU befinden. Wann dies der Fall ist, muss anhand von Hilfsfaktoren und Indizien bestimmt werden. Keine ausreichenden Anhaltspunkte hierfür sind etwa allein

- die bloße Abrufbarkeit einer kommerziellen Internetpräsenz, einer E-Mail-Adresse oder sonstiger Kontaktdaten oder
- die Verwendung einer (EU-)Sprache, die in dem Drittstaat, in dem das jeweilige Unternehmen niedergelassen ist, allgemein gebräuchlich ist.

Haftungsausschlüsse (so genannte Disclaimer), die beispielsweise die Anwendbarkeit der DS-GVO beschränken oder ausschließen, lassen wiederum nicht zwingend auf die Nichtanwendbarkeit der DS-GVO schließen.

Andere Faktoren wie

- die Verwendung der Sprache oder Währung eines Mitgliedstaates in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen oder
- die Erwähnung von Kunden oder Nutzern, die sich in der EU befinden,

können darauf hindeuten, dass ein Unternehmen beabsichtigt, den betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten (vgl. ErwGr. 23). Ein Angebot kann auch dann (potenzielle) Kunden und Nutzer in der EU adressieren, wenn das jeweilige Waren- oder Dienstleistungsangebot einen hinreichend konkreten perso-

nenal Bezug zum Marktgeschehen aufweist. Zur Bestimmung dessen können beispielsweise „Flaggen-Icons“, landesspezifische „Top Level Domains“ oder geographische Referenzen zu den mitgliedstaatlichen Märkten herangezogen werden.

2. Anknüpfungspunkt: Überwachung des Verhaltens von Personen (Art. 3 Abs. 2 lit. b DS-GVO)

Die DS-GVO ist auch dann anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten von betroffenen Personen zu beobachten, soweit dieses Verhalten in der EU erfolgt. Dies ist zum Beispiel dann der Fall, wenn die Internetaktivitäten der betroffenen Person nachvollzogen werden. Eine solche Nachvollziehbarkeit kann auch im Fall der nachfolgenden Erstellung von (Persönlichkeits-)Profilen angenommen werden, wenn

- diese die Grundlage für eine die jeweilige Person betreffende Entscheidung bilden oder
- anhand derer die Vorlieben, Verhaltensweisen oder Gepflogenheiten einer natürlichen Person analysiert oder vorausgesagt werden sollen (vgl. ErwGr. 24).

Dies kann zum Beispiel durch den Einsatz von „Tracking-Cookies“ oder „Browser Fingerprints“ stattfinden. Diese Techniken können auch als Grundlage für die weitere Erstellung persönlicher Profile, etwa zum Zwecke individualisierter bzw. zielgruppenspezifischer Werbung (sog. Behavioural Targeting) dienen.

Weitere Folgen

Außereuropäische Unternehmen, auf deren Verarbeitungstätigkeiten die DS-GVO anwendbar ist, müssen grundsätzlich einen in einem betroffenen Mitgliedstaat niedergelassenen Vertreter benennen. Der Vertreter ist ausdrücklich zu bestellen und schriftlich zu beauftragen, in Bezug auf die sich aus der DS-GVO ergebenden Pflichten an Stelle des Verantwortlichen oder des Auftragsverarbeiters zu handeln. Als Anlaufstelle soll dieser Vertreter einerseits den betroffenen Personen ermöglichen, ihre Betroffenenrechte wirksam geltend zu machen und andererseits die Aufsichtsbehörden in die Lage versetzen, ihre Aufsichtsmaßnahmen effektiv durchzusetzen (Art. 27 DS-GVO, siehe auch ErwGr. 80). Die Pflicht entfällt, wenn die Verarbeitung

- lediglich gelegentlich erfolgt,
- nicht die umfangreiche Verarbeitung sensibler personenbezogener Daten im Sinn von Art. 9 DS-GVO einschließt,
- nicht die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) einschließt und
- nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Der Verstoß gegen die Pflicht zur Bestellung ist bußgeldbewehrt (vgl. Art. 83 Abs. 4 lit. a DS-GVO).

Fazit

Auch Unternehmen, die keine Niederlassung in der EU haben, aber auf dem europäischen Markt tätig sind, müssen die DS-GVO voll anwenden. Darüber hinaus sind diese Unternehmen grundsätzlich verpflichtet, einen Vertreter in der EU zu benennen. Der europäische Gesetzgeber stellt die Aufsichtsbehörden mit Einführung des Marktortprinzips vor die nicht zu unterschätzende Herausforderung, den Geltungsanspruch der DS-GVO gegenüber Unternehmen in Drittstaaten durchzusetzen.

Anlage 15

Kurzpapier Nr. 8
Maßnahmenplan „DS-GVO“ für Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung

Die DS-GVO, die im Mai 2016 in Kraft getreten ist, wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Anders als die bisherige EU-Richtlinie wird diese EU-Verordnung ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und wird das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen. Gleichzeitig sieht das deutsche Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) eine ergänzende Neufassung des nationalen Rechts vor (z. B. BDSG-neu), soweit in der DS-GVO Spielraum für nationale Regelungen besteht. Viele Unternehmen sind aber noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die unabhängigen Datenschutzbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Information der Geschäftsleitung

Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet. In einem ersten Schritt ist daher von den betrieblichen Datenschutzbeauftragten und/oder den IT-Verantwortlichen die Geschäftsleitung zu informieren.

Start eines Projekts zur Umsetzung der DS-GVO

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind dahingehend zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DS-GVO gibt. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in einem Unternehmen. Da folglich verschiedene Personen bzw. Abteilungen im Unternehmen beteiligt sind, die untereinander koordiniert werden müssen, bietet es sich an, ein Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren.

Die Kernaufgabe wird dabei sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

1. Bestandsaufnahme

Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell realisierten Rahmenbedingungen aller Datenverarbeitungen analysiert werden (Ist-Zustand). Dies betrifft u. a.

- die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden (bestehende Dokumentationen, bspw. ein Verfahrensverzeichnis, können hierfür einen Ausgangspunkt bilden),
- die dazugehörigen Rechtsgrundlagen (die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn entweder ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat),
- die Datenschutzorganisation (d. h. alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),
- die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
- die Dokumentation (z. B. Verfahrensverzeichnisse, Vorabkontrollen, Datenschutzkonzepte, IT-Sicherheitskonzepte, Sicherheitsvorfälle) und
- sofern vorhanden Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

2. Handlungsbedarf eruieren

Nunmehr ist der Soll-Zustand zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchzuführen. Dabei sind u. a. folgende Punkte vor dem Hintergrund der DS-GVO zu beachten (zu den einzelnen Themen erscheinen weitere Kurzpapiere):

- **Rechtsgrundlagen:**

Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützt, ist zu prüfen, ob die Anforderungen des Art. 7 DS-GVO erfüllt sind (bei Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft ist zudem Art. 8 DS-GVO zu beachten).

- **Betroffenenrechte:**

Den betroffenen Personen stehen umfangreiche Rechte zu, die der Verantwortliche zu beachten hat (z. B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS-GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).

- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:**

Die DS-GVO enthält spezifische Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Data Protection by design und Data Protection by default).

- **Dienstleistungsbeziehungen:**

Dabei sollten insbesondere die bestehenden Verträge zur Auftragsverarbeitung überprüft werden. Die Art. 28 und 29 DS-GVO enthalten Vorgaben für Vereinbarungen mit Auftragsverarbeitern.

- **Dokumentationspflichten:**

Die DS-GVO verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Zusatz-

lich sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z. B. für das Verarbeitungsverzeichnis in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 lit. a DS-GVO).

- **Datenschutz-Folgenabschätzung:**

Die aus dem BDSG bekannte Vorabkontrolle wird durch die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO abgelöst und erfordert eine umfangreiche Dokumentation. Die Datenschutz-Folgenabschätzung kann zudem eine Konsultation der Aufsichtsbehörde nach sich ziehen (Art. 36 DS-GVO).

- **Meldepflichten:**

Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO).

- **Datensicherheit:**

Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten und die dafür implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).

- **Zertifizierung:**

Schlussendlich besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

3. Umsetzung bis zum 25. Mai 2018

Bei der Umsetzung sind dann u. a. folgende Punkte wieder zu beachten:

- Anpassung der betroffenen Prozesse und Strukturen,
- Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt),
- Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten,
- Anpassung der Datenschutzorganisation,
- ggf. Bestellung eines Datenschutzbeauftragten,

- Reaktionsmechanismen auf Datenpannen,
- Organisation von Meldepflichten,
- Anpassung der Dienstleistungsbeziehungen,
- Aufbau der Dokumentation,
- Anpassung der IT-Sicherheit und
- ggf. Anpassung der Betriebsvereinbarungen.

Anlage 16

Kurzpapier Nr. 9
Zertifizierung nach Art. 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Sinn und Zweck von Zertifizierungen

Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: „Woher weiß man, ob datenschutzrechtliche Vorgaben von einem Unternehmen oder einer Behörde eingehalten werden?“. Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifizierungen nachweisen zu lassen. Mit den Artikeln 42 und 43 der DS-GVO legt der Gesetzgeber einen rechtlichen Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Bisherige Erfahrungen der Aufsichtsbehörden

Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar, inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Förderung von Zertifizierungen

Einleitend weist Art. 42 Abs. 1 DS-GVO darauf hin, dass unter anderem auch die Aufsichtsbehörden auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutz-

siegeln und -prüfzeichen fördern sollen. Diese dienen dazu, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bis es jedoch so weit ist, dass die Verordnung umgesetzt und angewandt werden kann, müssen die Mitgliedstaaten in einer engen Zusammenarbeit die in der DS-GVO geforderten Mechanismen und Kriterien entwickeln. Dies ist zeitlich, räumlich und kapazitiv eine große Herausforderung für alle Beteiligten.

Vorteile einer Zertifizierung

Die DS-GVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

- Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f)
- Datenschutz-Folgeabschätzung (ErwGr. 90)

Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

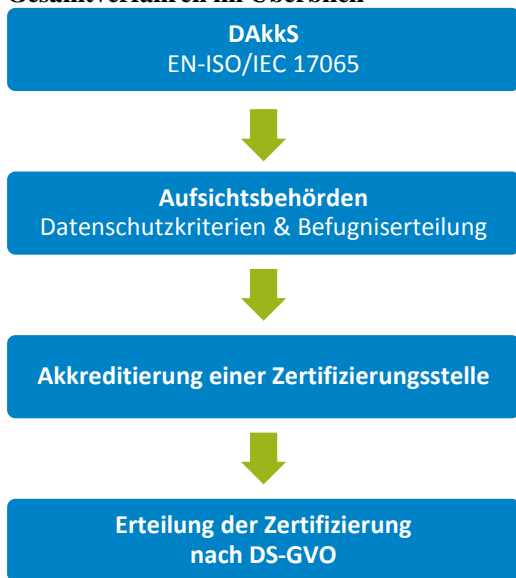
Einhaltung der DS-GVO – auch mit Zertifikat

Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ebenso verdeutlicht Art. 42 Abs. 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Zertifizierungsstellen

Nach Art. 42 Abs. 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 Akkreditierung DSAnpUG („BDSG-neu“) vor. Die Kriterien für die Akkreditierung werden von den Aufsichtsbehörden entwickelt und beruhen u. a. auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der beiden Parteien in einem eigens dafür eingerichteten Ausschuss ist Voraussetzung für die Akkreditierung einer Zertifizierungsstelle. Erst danach und nach der Erteilung der Befugnis durch die zuständige Aufsichtsbehörde, kann die Zertifizierungsstelle tätig werden. Sie darf im Anschluss, nach entsprechender Prüfung der Einhaltung der DS-GVO, Zertifizierungen erteilen.

Gesamtverfahren im Überblick



Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss die zu zertifizierende Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und

Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die bereits jetzt Informationssicherheit leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen

Art. 42 Abs. 7 DS-GVO weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die bei Erfüllung der einschlägigen Voraussetzungen verlängert werden kann. Die zuständige Zertifizierungsstelle und die Aufsichtsbehörde können die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung

Ausblick zu Datenschutz-Zertifizierungen

Zertifizierungen nach der DS-GVO bieten das Potenzial, künftig bei Verarbeitungsvorgängen (u. a. bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Cloud-Dienste entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einem bestimmten Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird. Ein Wildwuchs zahlreicher unterschiedlicher Zertifizierungsverfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.

Anlage 17

Kurzpapier Nr. 10

Informationspflichten bei Dritt- und Direkterhebung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung der Informationspflichten

Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmegvorschriften greifen.

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 (**Dritterhebung**, Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Information 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 lit. c DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem anderen Empfänger offenbaren möchte.

Informationspflichten bei Direkterhebung

Bei der Informationspflicht im Falle der **Direkterhebung** wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbei-

tung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).

- Name (ggf. Firmenname gem. § 17 Abs. 1 HGB oder Vereinsname gem. § 57 BGB) und Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreter
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und zusätzlich die Rechtsgrundlage, auf der die Verarbeitung fußt
- das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht (Art. 6 Abs. 1 lit. f DS-GVO)
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (vgl. Art. 4 Nr. 9 DS-GVO)
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und zugleich Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind)

Zusätzlich sind nach Abs. 2 Informationen über

- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkung- und Wider 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 einer Aufsichtsbehörde,
- ggf. die gesetzliche oder vertragliche Verpflichtung des Verantwortlichen, personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich Profiling) aussagekräftige Informationen über die

verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung zur Verfügung zu stellen.

Informationspflichten bei Dritterhebung

Auch im Falle einer **Dritterhebung** unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und 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 bzw. der zur Verfügung zu stellenden 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 personenbezogene Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 lit. d DS-GVO verpflichtet, die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für den 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 lit. 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 lit. f DS-GVO) nicht – wie bei der Direkterhebung – unter Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 lit. b DS-GVO).

Zweckänderung und Übermittlung

Die Informationspflichten im Falle einer Zweckänderung gelten sowohl für die Direkterhebung als auch für die Dritterhebung. Neben der Information über die geänderte Zweckbestimmung sind alle Informationspflichten gemäß Art. 13 Abs. 2 DS-GVO (Direkterhe-

bung) oder gemäß Art. 14 Abs. 2 DS-GVO (Dritterhebung) erneut zu erfüllen.

Die Übermittlung an einen Dritten ist häufig eine Zweckänderung, so dass schon aus diesem Grund vor der Übermittlung die betroffene Person entsprechend zu informieren ist. Darüber hinaus stellt Art. 14 Abs. 3 lit. c DS-GVO klar, dass bei der Offenlegung an einen neuen Empfänger (einschließlich Auftragsverarbeitern, vgl. Art. 4 Nr. 9 DS-GVO) informiert werden muss, soweit dieser nicht von der bereits nach Artikel 13 Abs. 1 lit. e DS-GVO erteilten Information über Empfänger oder Empfängerkategorien umfasst ist.

Zeitpunkt der Erfüllung der Informationspflichten

Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.

Im Falle der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den spezifischen Umständen, darf aber einen Monat nicht überschreiten. Die Monatsfrist ist eine Maximaldauer und sollte nicht pauschal angesetzt werden. 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.

Ausnahmen

Die Informationspflichten nach den Art. 13 und 14 DS-GVO bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Im Falle der Dritterhebung bestehen darüber hinaus keine Informationspflichten, wenn die Informationserteilung sich z. B. als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.

Außerdem sind in den §§ 32 und 33 des neuen Bundesdatenschutzgesetzes (BDSG-neu) weitere Ausnahmen von den Informationspflichten normiert. Die Informationspflicht nach Art. 13 DS-GVO soll beispielsweise gem. § 32 Abs. 1 Nr. 4 BDSG-neu nicht beste-

hen, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Es bestehen jedoch Zweifel, ob die in den §§ 32 und 33 BDSG-neu vorgesehenen Beschränkungen der Informationspflichten nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in den §§ 32 und 33 BDSG-neu vorgesehene Beschränkung der Informationspflichten aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Form der Informationspflicht

Gemäß Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen. Wird aber auf eine elektronisch verfügbare Information Bezug genommen, dann muss diese leicht auffindbar sein. Hierbei können auch Bildsymbole hilfreich sein.

Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. Dies gilt gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg.

Nachweise der Informationspflichten

Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 lit. a und Abs. 2 DS-GVO).

Folgen eines Verstoßes

Der Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 5 lit b DS-GVO mit einer Geldbuße bestraft werden.

Empfehlung

Es ist für Verantwortliche im eigenen Interesse ratsam, rechtzeitig die nach Art. 25 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

Anlage 18

Kurzpapier Nr. 11**Recht auf Löschung / „Recht auf Vergessenwerden“**

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Mit dem Inkrafttreten der DS-GVO erfährt die Löschung personenbezogener Daten gegenüber der bisherigen Rechtslage insofern eine Aufwertung, als die diesbezüglichen Bestimmungen detaillierter ausformuliert worden sind und zum Teil auch darüber hinausgehen. Das mit dem Löschungsanspruch der betroffenen Person verbundene „Recht auf Vergessenwerden“ wird zum ersten Mal ausdrücklich gesetzlich geregelt; es ergänzt die Löschung unmittelbar beim Verantwortlichen und die bereits bislang im BDSG verankerten Nachberichtspflichten.

Löschungspflicht

Wie aktuell in § 35 Abs. 2 BDSG-alt vorgesehen, bestimmt auch Art. 17 Abs. 1 DS-GVO, dass personenbezogene Daten auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich gelöscht werden müssen. Art. 17 Abs. 1 DS-GVO benennt dazu folgende Fälle:

- a) Die Notwendigkeit der Verarbeitung zur Zweckerreichung ist entfallen.
- b) Die betroffene Person hat ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage.
- c) Die betroffene Person legt gem. Art. 21 Abs. 1 oder 2 DS-GVO Widerspruch gegen die Verarbeitung ein; im Falle des Art. 21 Abs. 1 gilt dies nur, soweit keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. Das Widerspruchsrecht

nach Art. 21 Abs. 1 DS-GVO besteht ausschließlich bei Verarbeitungen, die auf Art. 6 Abs. 1 lit. e oder f DS-GVO gründen. Für die Löschungsverpflichtung bedarf es dabei einer Interessenabwägung. Anders bei Widersprüchen in Bezug auf Direktwerbung (Art. 21 Abs. 2 DS-GVO): Hier bedarf es keiner Interessenabwägung.

- d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

Der Verweis auf Art. 8 Abs. 1 DS-GVO (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) impliziert, dass die Daten rechtmäßig erhoben wurden. Eine Löschungspflicht ergibt sich damit allein aufgrund des Löschungsverlangens der betroffenen Person. Weil Diensten der Informationsgesellschaft (z. B. Soziale Netzwerke, Online-Spiele) in Bezug auf Minderjährige weniger Schutzbedarf als den betroffenen Personen zugestanden wird, bedarf es neben dem Löschungsverlangen keiner weiteren Voraussetzung; auch kann dieser Anspruch noch als Erwachsener geltend gemacht werden.

Recht auf Vergessenwerden

Das „Recht auf Vergessenwerden“ gem. Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung“ verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, einer breiten Öffentlichkeit zugänglich sind.

Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zu deren Löschung verpflichtet ist, hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten

oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Danach zieht der berechtigte Löschantrag einer betroffenen Person bzw. die bestehende Löschungspflicht eines Verantwortlichen dessen Pflicht nach sich, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über ein Verlangen des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren. Das Unterlassen entsprechender Bemühungen wird angesichts des Wortlauts der Norm und der fortlaufenden technischen Entwicklung nicht mit einem einfachen Verweis des Verantwortlichen auf unzumutbaren Aufwand begründet werden können.

Ausnahmen von der Löschungspflicht

Die Pflicht zur Löschung nach Art. 17 Abs. 1 und die Pflicht zur Information weiterer Verantwortlicher nach Art. 17 Abs. 2 DS-GVO entfallen, wenn gemäß Art. 17 Abs. 3 DS-GVO die Verarbeitung erforderlich ist

- a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- b) zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt;
- c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt;
- e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Allerdings berechtigen die benannten Ausnahmen nicht zu einer zeitlich unbegrenzten Verarbeitung der jeweiligen personenbezogenen Daten. Auch diese Zwecke werden zu einem bestimmten Zeitpunkt erfüllt und die Verarbeitung der Daten wird zur Zweckerreichung nicht mehr erforderlich sein. Dann sind auch diese Daten zu löschen.

Nachberichtspflichten

Die bislang schon bestehenden Nachberichtspflichten zur Löschung (§ 35 Abs. 7 BDSG-alt) bleiben bestehen. Art. 19 DS-GVO verpflichtet den Verantwortlichen, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Beschränkung des Lösungsanspruchs

Art. 23 DS-GVO befugt die Union und die Mitgliedstaaten, die Löschung gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, eine notwendige und verhältnismäßige Maßnahme darstellt und (zumindest) einem der in Art. 23 Abs. 1 lit. a bis j DS-GVO genannten Zwecke dient. Hiervon hat der Bundesgesetzgeber in § 35 BDSG-neu Gebrauch gemacht: Im Fall nicht automatisierter Datenverarbeitung und unter den weiteren dort genannten Voraussetzungen ist statt des Lösungsanspruchs der betroffenen Person ein Anspruch auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO vorgesehen.

Anwendbarkeit der Regelungen des BDSG-neu

Es bestehen jedoch Zweifel, ob die in § 35 BDSG-neu vorgesehenen Beschränkungen des Rechts auf Löschung nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in § 35 BDSG-neu vorgesehene Beschränkung des Rechts auf Löschung aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Sanktionen

Bei Verstößen gegen die Lösungs- oder Nachberichtspflichten droht die Einleitung eines Bußgeldverfahrens (Art. 83 Abs. 5 lit. b DS-GVO).

Abkürzungsverzeichnis

Abs.	Absatz
ADV	Auftragsdatenverarbeitung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
AMD	Arbeitsmedizinischer Dienst
AöR	Anstalt des öffentlichen Rechts
ArbMedVV	Verordnung zur arbeitsmedizinischen Vorsorge
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
Aufl.	Auflage
Az.	Aktenzeichen
BayLfDI	Bayerischer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
BDSG	Bundesdatenschutzgesetz
bDSG	behördlicher Datenschutzbeauftragter/ betrieblicher Datenschutzbeauftragter
BGB	Bürgerliches Gesetzbuch
BI	Bürgerinitiative
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
ca.	zirka
ChemVerbotsV	Chemikalien-Verbotsverordnung
d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle GmbH
DSFA	Datenschutz-Folgenabschätzung

DS-GVO	Datenschutz-Grundverordnung
e. V.	eingetragener Verein
EU	Europäische Union
EU-DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
EU-DS-GVO	Europäische Datenschutzgrundverordnung
EWR	Europäischer Wirtschaftsraum
GastG	Gaststättengesetz
gem.	gemäß
GesDV	Gesundheitsdienstverordnung
ggfs.	gegebenenfalls
GPS	Global-Positioning-System
grds.	grundsätzlich
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
HS	Halbsatz
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
InsO	Insolvenzordnung
Kfz	Kraftfahrzeug
Kita	Kindertageseinrichtung
KUG	Kunsturhebergesetz
LfD SL	Landesbeauftragter für den Datenschutz Saarland
LG	Landgericht
LPI	Landespolizeiinspektion
LRA	Landratsamt
Mio.	Millionen
Nr.	Nummer

NRW	Nordrhein-Westfalen
NSL	Notrufserviceleitstelle
o. g.	oben genannte/r/s
OVG	Oberverwaltungsgericht
PAuswG	Personalausweisgesetz
PC	Personalcomputer
PI	Polizeiinspektion
Rn.	Randnummer
s. a.	siehe auch
sog.	sogenannte(s,r)
StGB	Strafgesetzbuch
SV	Stadtverwaltung
ThürDSG	Thüringer Datenschutzgesetz
ThürSpiel- hallenG	Thüringer Spielhallengesetz
ThürVwVf G	Thüringer Verwaltungsverfahrensgesetz
ThürWTG	Thüringer Gesetz über betreute Wohnformen und Teilhabe
TKG	Telekommunikationsgesetz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TOMs	technische und organisatorische Maßnahmen
TPG	Thüringer Pressegesetz
u. a.	unter anderem
u. ä.	und ähnliches
u. U.	unter Umständen
UAbs.	Unterabsatz
usw.	und so weiter
UVV	Unfallverhütungsverordnung
VG	Verwaltungsgericht
vgl.	vergleiche

z. B.	zum Beispiel
ZB	Zwischenbericht
ZPO	Zivilprozessordnung

Stichwortverzeichnis/ Index

(DS-GVO	12.3
§ 201 StGB.....	6.32
§ 28 BDSG.....	3.44
§ 42a.....	5.1
66399.....	3.29
Abgabenordnung.....	3.32, 3.22
Abrufverfahren.....	4.4
Abschleppdienst	3.6
Abwägung 12.7, 9.1, 7.22, 7.18, 7.1, 6.69, 6.64, 6.62, 6.58, 6.38, 6.37, 6.27, 5.1, 3.45	
Adresse 12.11, 12.7, 12.6, 10.19, 10.16, 10.9, 6.36, 6.31, 6.30, 6.20, 6.14, 5.1, 4.3, 3.46, 3.45, 3.44, 3.42, 3.40, 3.26, 3.20, 3.19, 3.18, 3.10, 3.9	
Akten.. 10.18, 10.11, 10.2, 7.6, 3.47, 3.42, 3.39, 3.34, 3.29, 3.26, 2.6	
Akteneinsicht	10.6, 10.2, 6.30, 3.42
Aktenlager.....	3.29, 3.1
Aktenvernichtung	10.18, 3.39, 3.34, 2.6
Alarm	6.10
allgemeines Persönlichkeitsrecht	6.62, 6.48, 6.46, 6.27, 6.26, 6.13
Altakten.....	3.47
Altenhilfe	7.6
Amtsarzt.....	10.16
Amtshandlung	6.57
Amtshilfe.....	6.57, 6.43, 6.12, 3.42, 3.1
Anlage	6.50
Anonymisierung.....	12.12, 7.22
Anordnung	6.46, 6.42, 6.37, 6.30, 6.10, 4.3, 3.32
Anpassungsgesetz zur EU-Datenschutz-Grundverordnung (EU- DSAnpUG-EU)	6.38
Anschrift 8.1, 6.12, 4.3, 4.2, 3.45, 3.44, 3.40, 3.36, 3.32, 3.26, 3.18, 3.14, 3.13, 3.12, 3.11, 3.6, 3.3, 3.2	
Ansteckung	10.1
Anwendungssoftware.....	4.5
Anzeigenerstatter	6.62
Apotheke.....	10.19, 10.9, 10.4, 10.3, 6.68
Apotheker.....	10.19, 10.9, 10.3, 6.68
App.....	12.15, 12.4, 10.22, 10.20, 10.5, 6.10, 6.3, 4.5, 3.33, 3.24
App-Entwicklung	4.5

Approbation	10.22
Arbeitgeber 10.2, 7.22, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.14, 7.13, 7.11, 7.9, 7.8, 7.5, 7.4, 7.2, 6.71, 6.28, 4.1, 3.25	
Arbeitnehmer	<i>Siehe Beschäftigte</i>
Arbeitnehmerdatenschutz	7.22, 6.9
Arbeitnehmerüberlassung	7.10
Arbeitsleistung	7.22, 7.15
Arbeitsplatzrechner	7.13
Arbeitsplatzüberwachung	6.71
Arbeitssicherheitsgesetz	10.2, 7.9
Arbeitsunfall	7.12
Arbeitsverhältnis	10.2, 7.22, 7.20, 7.19, 7.8, 2.2
Arbeitsvermittlung	7.19, 7.8
Arbeitsvertrag	7.17, 7.9
Arbeitszeit	7.17, 7.15
Armaturenbrett	6.62
Art der Daten	3.30
Arzt	10.22, 10.15, 10.14, 10.11, 10.10, 10.6, 10.1, 7.9, 7.9, 3.26
Arztpraxis	10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 5.1, 3.26
Attest	10.16
Attrappe 6.68, 6.67, 6.56, 6.55, 6.54, 6.51, 6.48, 6.43, 6.35, 6.34, 6.27, 6.22, 6.19, 6.16	
Aufbewahrungsfrist	10.18
Aufbewahrungsfriste	7.6
Aufgaben 12.8, 10.16, 10.4, 10.2, 7.6, 7.5, 6.68, 6.57, 6.32, 6.17, 4.2, 3.36, 3.30, 3.18, 2.5, 2.4, 2.3, 2.2	
Aufnahmebereich 7.5, 6.71, 6.68, 6.64, 6.56, 6.53, 6.50, 6.43, 6.32, 6.27, 6.23, 6.21, 6.11, 6.8, 6.5	
Aufsichtsbehörde 12.9, 12.6, 12.1, 11.1, 10.12, 10.11, 10.5, 10.4, 10.2, 7.5, 7.3, 6.68, 6.42, 6.41, 6.40, 6.39, 6.38, 6.37, 6.32, 6.27, 6.24, 6.21, 6.20, 6.18, 6.14, 6.12, 6.11, 6.9, 6.3, 6.2, 5.1, 4.3, 3.41, 3.35, 3.21, 3.20, 3.18, 3.3, 3.2, 2.6, 2.5	
Auftragsdatenverarbeitung 12.6, 10.18, 10.12, 10.5, 3.47, 3.39, 3.34, 3.24, 3.5, 2.1	
Aufzeichnung 10.20, 10.2, 7.17, 7.1, 6.74, 6.64, 6.62, 6.58, 6.50, 6.41, 6.40, 6.29, 6.28, 6.23, 6.23, 6.20, 6.13, 6.13, 6.8, 6	
Auskunft 10.13, 10.11, 10.6, 10.5, 10.3, 10.2, 9.3, 9.2, 9.1, 8.2, 8.1, 7.18, 7.16, 7.15, 7.11, 7.10, 7.8, 7.7, 6.68, 6.67, 6.44, 6.43, 6.42, 6.30, 6.29, 6.28, 6.27, 6.17, 6.12, 6.10, 4.5, 3.43, 3.42, 3.31, 3.25, 3.23, 3.23, 3.19, 3.15, 3.13, 3.8, 3.7	

Auskunftei	9.2, 9.1, 3.19
Auskunfteiabfrage	9.2, 9.1
Auskunftsanspruch	8.1, 3.43, 3.7
Auskunftsbescheid	6.42
Auskunftsersuchen 10.6, 10.3, 9.3, 8.2, 7.20, 7.1, 6.76, 6.75, 6.74, 6.69, 6.68, 6.64, 6.52, 6.45, 6.42, 6.36, 6.30, 6.28, 6.27, 6.9, 6.8, 6.7, 6.4, 3.43, 3.36, 3.27, 3.17, 3.13, 3.7, 3.3	
Auskunftserteilung	6.17, 6.14, 3.23
Auskunftspflicht	8.2, 7.10, 6.63, 6.32, 3.43, 3.13
Auskunftsrecht	12.4, 9.3, 7.10, 6.26
Auskunftsverlangen 10.11, 10.7, 9.3, 7.21, 7.10, 7.4, 6.71, 6.63, 6.53, 6.50, 6.48, 6.47, 6.46, 6.44, 6.35, 6.16, 6.6, 6.5, 4.3, 3.45, 3.43, 3.16, 3.7, 3.2	
Auskunftsverweigerung	6.17, 3.23
Ausland	3.42, 3.30, 3.20
außereuropäisches Ausland	3.30, 1
Ausweichfläche	6.48
Ausweiskopie	3.14, 3.12, 3.6
Authentifizierung	12.10, 12.8, 10.5, 2.7
Auto	12.4, 6.62, 6.54, 3.6
Autohaus	6.59, 6.31, 3.7, 3.6
automatisierte Verarbeitung 7.18, 7.5, 6.58, 6.39, 6.28, 6.21, 6.9, 6.2, 3.2, 2.6, 2.5, 2.1	
Bade- und Ruhebereich	6.40
Bank	9.1, 9.1, 5.1, 3.44, 3.44, 3.35, 3.23, 3.23, 3.22, 3.22
Baumarkt	3.10
Bauordnungsamt	3.42
Baustelle	6.11
Baustellenkamera	6.11
bDSB	3.42, 3.30, 2.6, 2.5, 2.3, 2.2, 2.1
Behandlungsfehler	10.8, 10.7
behinderte Menschen	7.14
Behördenebene	6.57
behördlicher Datenschutzbeauftragter	13.2, 3.42, 3.30, 2.1
Beitragszahlung	3.25
Beobachtung 7.17, 7.1, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.64, 6.62, 6.61, 6.60, 6.58, 6.54, 6.50, 6.48, 6.44, 6.41, 6.40, 6.36, 6.35, 6.29, 6.23, 6.20, 6.15, 6.14, 6.13, 6.11, 6.8, 6.7, 6.6, 6.3, 2.1	
Beobachtungsbefugnis 6.66, 6.58, 6.54, 6.53, 6.50, 6.48, 6.44, 6.33, 6.31, 6.24, 6.23, 6.21, 6.16	

Beobachtungskamera	6.63
Beratung	10.16, 10.6, 7.17, 7.12, 6.55, 6.51, 6.14, 4.1, 3.41, 2.4
Beratung durch den TLfDI	7.12, 6.41
Beratungsersuchen gem. § 38 Abs. 1 Satz 2 BDSG	2.4
berechtigte Interessen 9.2, 8.1, 7.17, 7.9, 7.5, 7.4, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.65, 6.64, 6.61, 6.60, 6.59, 6.58, 6.53, 6.48, 6.44, 6.40, 6.38, 6.37, 6.36, 6.35, 6.34, 6.31, 6.29, 6.28, 6.27, 6.26, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 4.3, 3.45, 3.37, 3.31, 3.28, 3.19, 3.15, 3.14, 3.8, 3.4, 3.3	
Berufsgeheimnis	10.6, 5.1, 3.34
Berufsgeheimnisträger	10.6, 10.3, 5.1, 3.34, 3.26
Beschädigungen 6.75, 6.59, 6.55, 6.53, 6.48, 6.44, 6.40, 6.27, 6.20, 6.16	
Beschäftigte 14, 10.17, 10.2, 7.22, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.14, 7.14, 7.13, 7.12, 7.11, 7.10, 7.9, 7.8, 7.5, 7.4, 7.2, 7.1, 6.71, 6.69, 6.28, 6.8, 6.6, 4.1, 3.30, 3.25, 2.3	
Beschäftigtendaten	7.20, 7.17, 7.16, 7.5, 4.1
Beschäftigtendatenschutz	7.16, 7.15, 7.4, 6.28, 6.8, 1
Beschäftigungsverhältnis	7.20, 7.18, 7.16, 7.15, 7.8, 6.28, 6.11
Bescheid	6.71, 6.30, 6.17, 3.15
Beschwerde 12.5, 10.21, 10.16, 10.15, 10.10, 10.9, 10.6, 10.4, 9.3, 8.1, 7.21, 7.20, 7.19, 7.18, 7.17, 7.10, 7.8, 7.7, 7.5, 7.3, 7.2, 6.74, 6.71, 6.68, 6.66, 6.64, 6.63, 6.57, 6.56, 6.54, 6.53, 6.52, 6.51, 6.50, 6.48, 6.44, 6.37, 6.36, 6.33, 6.31, 6.30, 6.29, 6.27, 6.26, 6.22, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.9, 6.8, 6.5, 6.4, 3.46, 3.44, 3.43, 3.36, 3.27, 3.22, 3.21, 3.20, 3.17, 3.16, 3.15, 3.13, 3.12, 3.11, 3.9, 3.8, 3.7, 3.6, 3.5, 3.2	
besondere Art personenbezogener Daten 10.18, 10.11, 10.10, 10.9, 10.5, 10.1, 6.37, 5.1, 3.41, 3.39, 3.37, 3.26, 3.4	
Bestattung	3.13
Bestattungsunternehmen	3.13
Bestattungswald	3.28
Bestellpflicht	3.30, 2.5, 2.1
Bestellung des DSB	2.5, 2.3, 2.2
Bestimmbarkeit	3.17
Besucher 7.1, 6.75, 6.74, 6.71, 6.69, 6.52, 6.48, 6.37, 6.27, 6.25, 6.23, 6.18, 6.15, 6.8, 6.4, 3.3	
Betäubungsmittelgesetz	6.5

Betreiber	12.10, 12.9, 12.7, 12.4, 12.2, 10.20, 10.5, 6.76, 6.75, 6.74, 6.67, 6.66, 6.65, 6.64, 6.63, 6.58, 6.56, 6.52, 6.50, 6.47, 6.44, 6.43, 6.42, 6.38, 6.32, 6.30, 6.29, 6.27, 6.26, 6.24, 6.22, 6.20, 6.19, 6.18, 6.14, 6.13, 6.9, 6.7, 6.6, 6.3, 6.1, 3.35, 3.19, 3.8
Betreuer	7.14
Betreuungseinrichtung	10.1
betrieblicher Datenschutzbeauftragter	13.2, 11.1, 10.2, 9.3, 7.5, 7.5, 7.4, 6.21, 6.9, 6.3, 3.23, 3.7, 3.2, 2.5, 2.4, 2.4, 2.3, 2.2
Betriebsarzt	10.2, 7.10
Betriebsarzdokumentation	10.2
Betriebsstätte	7.21, 7.16, 3.23, 3.20
Betriebsvereinbarung	7.18
Bewegungsmelder	6.62, 6.7
Bewegungsprofil	7.22, 7.18, 7.11, 6.18
Beweiserheblichkeit	6.62
Beweismittel	6.62, 6.57
Beweissicherung	7.5, 6.71, 6.66, 6.62, 6.50, 6.36, 6.4, 6.3
Beweissicherungsinteresse	6.62
Bewerber	7.21, 3.7
Bewerbers	7.20
Bewerbung	7.21, 7.20, 7.19, 7.10, 7.8, 7.7, 3.7
Bewerbungsunterlagen	7.21, 7.20, 7.19, 7.10
Bewerbungsverfahren	7.7, 3.7
Biergarten	6.6
Bildauflösung	6.25
Bilder	7.14, 7.12, 6.75, 6.64, 6.62, 6.57, 6.52, 6.51, 6.50, 6.38, 6.29, 6.28, 6.23, 6.20, 6.19, 6.18, 6.13, 6.11, 6.9, 6.3, 6.2, 3.6
Biometrie	12.10
Black-Box-Verfahren	6.40, 6.38
Black-List	2.6
Blickwinkel	6.62, 6.23, 6.14
Bluetooth	12.15, 12.3
Bombenbau	3.14
Bonitätsabfrage	9.2, 3.19
Bonitätsprüfung	3.19
Botnetz	12.11
BSI	12.13, 12.11, 12.8, 10.5, 7.13, 2.2
BSI-Gesetz	12.9
BSI-Kritisverordnung	12.9, 12.2
Bundesmeldegesetz	3.11

Bundesnetzagentur	12.15, 12.9, 12.8, 8.1
Bundesverfassungsgericht	6.62, 6.48, 6.34, 6.13, 1
Büro	7.3, 6.66, 6.32, 6.28, 6.8
Büroeingang	6.66
Bußgeldtatbestand	6.2
Bußgeldverfahren 11.1, 10.9, 7.19, 7.5, 7.2, 6.69, 6.62, 6.44, 6.32, 6.30, 6.24, 6.19, 6.17, 6.2, 6.1, 2.4, 1	
Campingplatz	6.29
Canvas-Blocker	12.12
Cayla	12.15
CDU	3.1
Checkliste	5.1
Cookie-Richtlinie	12.3
Dachverband	4.2, 3.18
Dashboardcams	6.62
Dashcams	6.62, 1
Data protection by default	12.4, 10.20
Datendiebstahl	10.4, 5.1
Datenerhebung 10.9, 9.2, 6.75, 6.71, 6.61, 6.7, 6.6, 6.4, 6.2, 6.1, 4.5, 4.1, 3.44, 3.40, 3.31, 3.28, 3.11, 3.10, 3.8, 3.6, 3.3, 3.2	
Datenermittlung	6.61
Datenpanne	5.1
Datenschutzbeauftragter 13.2, 12.13, 12.10, 12.7, 12.5, 12.3, 12.1, 10.18, 10.14, 10.13, 10.12, 10.6, 10.2, 9.3, 7.15, 7.12, 7.5, 7.3, 6.32, 6.28, 6.24, 6.9, 6.3, 3.37, 3.30, 3.23, 3.22, 3.20, 3.18, 2.6, 2.5, 2.4, 2.4, 2.3, 2.2, 2.1	
Datenschutz-Folgenabschätzung	10.12, 2.6, 2.1
Datenschutz-Grundverordnung 13.2, 12.3, 11.1, 10.12, 6.72, 6.60, 6.41, 6.40, 6.38, 6.1, 2.6, 2.1, 1	
datenschutzrechtliche Einwilligungserklärung	3.40, 3.11
Datenträgervernichtung	10.13, 2.6
Datenübermittlung 10.16, 10.14, 10.6, 7.9, 4.4, 4.2, 3.45, 3.40, 3.37, 3.30, 3.28, 3.26, 3.18, 3.8, 3.4, 1	
Datenübertragung	10.5
Datenverarbeitung im Auftrag	10.18, 7.8, 6.27, 3.5
Datenweitergabe	4.2, 3.28, 3.26, 3.18
Deutsche Post AG	3.48
Deutscher Presserat	3.21
Diebstahl	7.4, 7.1, 6.59, 6.53, 6.50, 6.29, 6.8, 6.6, 6.5, 5.1, 2.7
Dienstkräfte	6.57

Dienstpläne	7.6, 2.7
digitale Unterschrift	3.38
digitaler Türspion	6.13
DIN 32757-1	3.34
DIN 66399	10.21, 10.18, 10.13
DIN 66399-1	3.39
DIN 66399-2	3.47
Diözesandatenschutzbeauftragter	3.48
Diskothek	6.76
Double-Opt-In	3.9
Drehkreuze	6.40, 6.37
DS-GVO 12.4, 12.1, 11.1, 10.20, 10.12, 6.72, 6.60, 6.41, 6.40, 6.38, 3.30, 2.6, 2.1, 1	
Durchsuchungsbeschluss	6.30
dynamische IP-Adresse	12.7
e-Datenschutz-Richtlinie	12.3
eID	12.13
eIDAS-Durchführungsgesetz	12.8
eIDAS-Verordnung	12.8
eigene Grundstück	6.54
eigenes Grundstück 6.75, 6.67, 6.66, 6.64, 6.58, 6.52, 6.43, 6.37, 6.33, 6.24, 6.23, 6.21, 6.18	
Eigentümer 12.11, 12.4, 6.75, 6.74, 6.55, 6.53, 6.47, 6.46, 6.45, 6.36, 6.35, 6.34, 6.33, 6.31, 6.29, 6.27, 6.20, 6.12, 6.7, 6.4, 3.47, 3.42, 3.8	
Eigentumsrecht	6.51
Einbrüche 7.5, 7.3, 6.67, 6.66, 6.59, 6.53, 6.50, 6.32, 6.29, 6.28, 6.27, 6.20, 6.16, 6.13, 6.10, 6.8, 6.7, 6.5, 5.1, 2.7	
Eingangs- und Kassenbereich	6.40
Eingangsbereich 7.3, 7.1, 6.76, 6.75, 6.74, 6.71, 6.67, 6.66, 6.45, 6.36, 6.27, 6.22, 6.18, 6.15, 6.13, 6.6, 6.4, 6.3	
Eingriff 12.9, 12.7, 7.21, 6.75, 6.74, 6.72, 6.72, 6.69, 6.68, 6.67, 6.65, 6.64, 6.62, 6.58, 6.56, 6.55, 6.48, 6.46, 6.41, 6.40, 6.34, 6.27, 6.26, 6.23, 6.13, 3.6, 3.4	
Einkaufen	6.3, 3.19
Einkaufszentrum	3.33
Einlasskontrolle	6.18, 6.13
Einrichtung 12.7, 12.4, 10.17, 10.1, 7.17, 7.14, 7.6, 6.76, 6.75, 6.72, 6.71, 6.70, 6.69, 6.64, 6.61, 6.60, 6.57, 6.44, 6.38, 6.35, 6.29, 6.21, 6.16, 6.13, 6.7, 6.3, 3.39, 2.7, 1	

Einsichtsrecht	10.6
Eintrittskarten	3.3
Einverständnis	10.7, 7.5, 6.71, 6.69, 6.64, 6.14, 3, 3.20, 3.16
Einwilligung 12.7, 12.4, 12.3, 10.16, 10.14, 10.9, 10.8, 10.7, 10.6, 10.3, 10.2, 10.1, 9.2, 7.22, 7.21, 7.20, 7.19, 7.14, 7.10, 7.9, 7.5, 7.3, 7.2, 6.75, 6.72, 6.71, 6.52, 6.44, 6.39, 6.34, 6.27, 6.23, 6.21, 6.20, 6.18, 6.15, 6.13, 6.12, 6.11, 6.8, 6.7, 6.6, 6.4, 6.2, 4.3, 4.2, 3.45, 3.44, 3.40, 3.38, 3.37, 3.33, 3.30, 3.28, 3.26, 3.25, 3.18, 3.17, 3.16, 3.15, 3.12, 3.11, 3.10, 3.9, 3.8, 3.3, 1	
Einwilligungserklärung 10.20, 10.14, 10.9, 7.21, 7.19, 7.14, 6.75, 6.69, 3.41, 3.40, 3.36, 3.26, 3.18, 3.11	
E-Learning-Plattform	12.10
Eltern	10.16, 7.14, 6.53
Entsorgung	10.21, 3.47, 3.34
e-Privacy-Richtlinie	12.3
e-Privacy-Verordnung	12.3
ERFA-Kreis	13.2
Erfassungsbereich 6.76, 6.71, 6.67, 6.58, 6.55, 6.52, 6.51, 6.49, 6.44, 6.43, 6.36, 6.34, 6.33, 6.27, 6.24, 6.23, 6.21, 6.16, 6.11, 6.3	
Erfassungsblatt Kameras	6.41
Erforderlichkeit 9.2, 7.22, 6.76, 6.75, 6.66, 6.64, 6.60, 6.58, 6.41, 6.40, 6.37, 6.23, 6.6, 6.4, 6.3, 4.3, 3.45, 3.14, 3.10, 3.3	
Erlaubnisnorm 12.4, 6.41, 6.23, 6.21, 6.18, 6.8, 6.7, 6.6, 3.44, 3.32, 3.31, 3.15, 3.11, 3.8, 3.3	
Etage	6.16, 3.45
EuGH C-212/13 (Rynes-Urteil)	6.37
Europäische Datenschutz-Grundverordnung	12.4, 6.38
externer Datenschutzbeauftragter	10.14, 7.4, 6.69, 3.7, 2.5, 2.4, 2.1
Facebook	12.5, 7.2, 5.1
Fachkunde	13.2, 7.5, 2.5, 2.4, 2.3, 2.2
Fahrgastbereich bzw. -raum	6.72
Fahrzeug 12.4, 7.11, 7.4, 6.75, 6.72, 6.62, 6.61, 6.54, 6.53, 6.38, 6.5, 3.6, 1	
familiäre und persönliche Tätigkeit	6.66, 6.52, 6.37, 6.23, 6.16
Familienversicherung	10.15
Fassade	6.55, 6.54, 6.50, 6.48, 6.17, 6.4
Fassadenteile	6.5
Fenster	6.66, 6.64, 6.50, 6.48, 6.16, 6.14, 2.7
Festlegung 10.18, 10.16, 10.2, 7.18, 7.17, 7.15, 7.11, 7.7, 7.4, 7.2, 6.41, 6.28, 6.5, 6.4, 6.3, 3.38, 2.7	

Filiale	7.16, 3.23, 3.22
Fingerprinting.....	12.12
Firmengelände.....	6.64, 6.60, 6.39, 6.28, 6.8
Firmensitz	6.8, 3.42
Firmenwagen.....	7.18, 7.11, 7.4
Fitnessstudio	7.3
Fitness-Tracker.....	10.20
Foto 12.5, 10.19, 10.8, 10.7, 7.21, 6.66, 6.61, 6.54, 6.50, 6.47, 6.30, 6.19, 6.16, 6.11, 3.42, 3.40, 3.29, 2.7	
Fotografie.....	10.8, 10.7, 6.12
Fotodokumentation	10.7, 6.57, 3.6
Fragenkatalog 6.68, 6.63, 6.53, 6.50, 6.48, 6.42, 6.22, 6.16, 6.5, 3.38	
Freiwilligkeit.....	12.4, 7.2, 6.71, 6.69, 6.11, 6.8, 6.6, 3.25
Freizeitpark	7.1
Friedhof.....	6.63
Fristsetzung	9.3, 6.17, 3.7
Garage	6.44, 6.24, 6.5
Garagenzufahrt.....	6.66
Garten.....	6.75, 6.67, 6.51, 6.23, 6.22, 6.4
Gartenanlage	6.49
Gäste . 7.1, 6.74, 6.72, 6.40, 6.37, 6.32, 6.29, 6.23, 6.6, 3.11, 3.8, 3.3	
Gastraum	6.74, 6.72, 6.6
Gaststätte.....	6.74, 6.29, 6.6
Gaststättengesetz.....	6.74
Gebäude 6.75, 6.69, 6.67, 6.66, 6.64, 6.55, 6.54, 6.53, 6.50, 6.48, 6.47, 6.46, 6.45, 6.44, 6.36, 6.34, 6.33, 6.30, 6.29, 6.28, 6.27, 6.22, 6.19, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.8, 6.7, 6.6, 6.4, 3.47, 3.42, 3.29, 3.14, 2.7	
Gebäudeservice	3.12
Geeignetheit	6.76, 6.28, 6.4
Gefahr für Leib und Leben.....	10.1
Gefährdung	12.2, 6.71, 6.53, 6.38, 6.27, 6.20, 6.5
Gefahrenlage 6.76, 6.75, 6.72, 6.71, 6.69, 6.53, 6.48, 6.38, 6.27, 6.20, 6.16, 6.13, 6.7, 6.5, 6.4	
Geheimnis	10.11, 10.10, 10.3, 10.1, 3.47, 3.39, 3.34, 3.26
Gehweg 6.76, 6.75, 6.67, 6.50, 6.48, 6.45, 6.44, 6.37, 6.24, 6.21, 6.20, 6.18, 6.16, 6.8, 6.4	
Geldbuße	11.1, 6.68, 6.63, 6.60, 3.7
Geldspielgeräte.....	6.71
Geldwäsche	3.22

Geldwäschegesetz	3.22, 3.12
Gemeindekindergarten	6.53
Geschäft des täglichen Lebens	4.1
Geschäftsbedingungen	9.2, 6.3, 3.5
gespeicherte Daten 10.13, 9.1, 8.2, 7.10, 7.8, 7.7, 6.32, 3.43, 3.23, 3.13, 3.7	
Gesundheit . 12.4, 12.2, 10.20, 10.19, 10.15, 10.14, 10.2, 10.1, 5.1, 1	
Gesundheit oder Freiheit von Personen	6.72, 6.61, 6.38
Gesundheitsdaten 10.20, 10.18, 10.13, 10.11, 10.10, 10.9, 10.6, 10.5, 10.1, 5.1, 3.39, 3.37, 3.26	
Gesundheitsverordnung.....	10.16
Gesundheitsvorsorge	10.2, 10.1
Gewerbeamt	6.7, 3.42
Gewerbetreibende	6.31, 6.5
Google Analytics.....	12.6
GPS	7.18, 7.11, 7.11, 7.4, 1
Graffiti.....	6.75, 6.55, 6.50, 6.44, 6.19, 6.5
Grenze 12.4, 6.69, 6.65, 6.62, 6.59, 6.58, 6.57, 6.53, 6.50, 6.44, 6.8, 3.31	
großflächige Anlagen des Personennahverkehrs.....	6.38
Grundbuchamt.....	6.47, 6.12
Grundrecht 12.11, 12.7, 12.4, 7.2, 6.67, 6.62, 6.55, 6.48, 6.34, 6.18, 6.16, 6.13, 6.3, 4.3, 1	
Grundstück 10.4, 6.67, 6.66, 6.64, 6.63, 6.58, 6.57, 6.56, 6.54, 6.53, 6.52, 6.51, 6.50, 6.49, 6.48, 6.46, 6.44, 6.43, 6.36, 6.34, 6.33, 6.32, 6.30, 6.24, 6.23, 6.22, 6.21, 6.20, 6.18, 6.17, 6.16, 6.14, 6.12, 6.8	
Grundstücksgrenze 6.64, 6.58, 6.54, 6.53, 6.51, 6.50, 6.48, 6.33, 6.31, 6.24, 6.23, 6.21, 6.16	
Grundstücksnutzer	6.53
Hacker-Angriff.....	12.14, 12.13, 12.11, 12.2, 5.1, 3.35
Handelsregistrauszug.....	6.31
Haus 12.11, 6.75, 6.67, 6.64, 6.55, 6.48, 6.43, 6.33, 6.30, 6.28, 6.27, 6.26, 6.20, 6.19, 6.18, 6.14, 6.4, 3.35, 3.27, 2.7	
Hauseingang.....	6.75, 6.52, 6.48, 6.43, 6.35, 6.27, 6.23, 6.22, 6.13
Hausgrundstück.....	6.51
Hausleitung	3.1
Hausrecht 7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.54, 6.53, 6.52, 6.50, 6.48, 6.44,	

6.40, 6.38, 6.37, 6.36, 6.35, 6.34, 6.32, 6.31, 6.29, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.11, 6.9, 6.8, 6.7, 6.4, 6.3	
Hausrechtsinhaber 6.54, 6.53, 6.50, 6.48, 6.44, 6.33, 6.24, 6.23, 6.21, 6.16	
Hausverwaltung	6.27, 3.45, 3.27
Hecke	6.49
Heimaufsicht	10.17
Hilfe	8.1, 7.12, 7.1, 6.57, 6.37, 6.1, 3.11, 2.5
Hinterbliebene	3.13
Hinweispflicht	6.62, 6.60, 6.36
Hinweisschild 7.3, 7.1, 6.60, 6.55, 6.52, 6.50, 6.46, 6.44, 6.36, 6.36, 6.23, 6.18, 6.13, 6.11, 6.8, 6.5	
Hotel	6.32, 3.11, 3.8
Identitätsbetrug	3.46
Imbisslokal	6.74
Immelborn	3.1
Inbetriebnahme .. 10.17, 7.5, 6.66, 6.51, 6.39, 6.33, 6.28, 6.9, 6.2, 3.2	
informationelle Selbstbestimmung 12.4, 7.22, 7.14, 6.72, 6.62, 6.55, 6.48, 6.34, 6.23, 6.23, 6.18, 6.11, 6.3, 3.17, 3.6, 3.6, 3.4, 1	
informationelles Selbstbestimmungsrecht 12.7, 10.10, 6.75, 6.74, 6.69, 6.67, 6.64, 6.58, 6.40, 6.38, 6.13, 3.26	
Infotainmentsysteme	12.4
Innenhof	6.66, 6.36, 6.31
Insolvenz	6.45, 6.12, 3.37, 3.26, 3.8
Insolvenzmasse	6.45, 6.12, 3.8
Insolvenzverwalter	6.45, 6.12, 3.26, 3.8
Interessen 10.1, 9.1, 7.22, 7.18, 7.17, 7.6, 7.5, 7.1, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.62, 6.61, 6.60, 6.58, 6.58, 6.54, 6.53, 6.52, 6.50, 6.48, 6.44, 6.41, 6.40, 6.38, 6.37, 6.36, 6.35, 6.29, 6.28, 6.27, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 5.1, 4.3, 3.45, 3.37, 3.31, 3.28, 3.4, 3.3, 2.5, 2.2	
Interessenabwägung	12.7, 6.72, 6.58, 3.45, 3.37, 3.4
Interessenkollision	2.5, 2.3, 2.2
Interessenkonflikt	10.6, 7.5, 2.5, 2.3, 2.2
Internethandel	3.35
Intimsphäre	6.69, 6.40
IT-Mitarbeiter	2.2
IT-Sicherheitsbeauftragter	2.3, 2.2
IT-Sicherheitsgesetz	12.2

Jäger	6.70, 6.58, 6.2
Jobcenter	7.10, 3.20
journalistisch-redaktionelle Zwecke	4.3, 3.21
juristische Person	6.18, 6.2, 4.4, 4.1, 3.46, 3.13, 2.5, 2.4, 2.1
Justiz	3.1
Kamera 7.17, 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.68, 6.67, 6.66, 6.65, 6.64, 6.63, 6.62, 6.61, 6.60, 6.58, 6.57, 6.56, 6.55, 6.54, 6.53, 6.52, 6.51, 6.49, 6.48, 6.47, 6.46, 6.45, 6.44, 6.43, 6.42, 6.41, 6.40, 6.38, 6.36, 6.35, 6.34, 6.33, 6.32, 6.31, 6.30, 6.29, 6.28, 6.27, 6.26, 6.25, 6.24, 6.24, 6.23, 6.22, 6.21, 6.20, 6.19, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.10, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2	
Kameraatrappe 6.67, 6.57, 6.56, 6.55, 6.54, 6.51, 6.48, 6.43, 6.42, 6.35, 6.34, 6.27, 6.22, 6.16	
Kamerasystem	6.5
Kasse	7.16, 6.74, 6.9, 3.44, 3.3
Kinder	12.15, 10.16, 10.11, 7.14, 6.53, 6.21
Kindergarten	6.53
Kindertageseinrichtung	2.7
kirchliche Stellen.....	3.20
Klageschrift.....	3.4
Klageverfahren.....	3.4
Klausel	10.12, 7.9, 2.2
Kleider- und Wertspindschließfächer.....	6.40
Klingel.....	6.52, 6.36, 6.23, 6.15, 6.13
Klingelkamera	6.15
kommunales Wettbewerbsunternehmen	4.1
Konkurrenzunternehmen.....	7.8
Kontaktdaten ... 10.19, 7.10, 7.1, 6.60, 6.55, 6.36, 6.23, 6.18, 4.3, 3.9	
Kontrolle 12.4, 10.18, 10.11, 10.4, 9.2, 7.22, 7.7, 7.5, 7.4, 6.72, 6.69, 6.68, 6.65, 6.64, 6.60, 6.59, 6.47, 6.36, 6.32, 6.27, 6.18, 6.8, 6.7, 3.44, 3.29, 3.20, 3.2, 2.5, 2.3	
Kopie.....	3.22, 3.14, 3.14, 3.12, 3.12, 3.7
Korruptionsbekämpfung	4.1
Kosten	12.11, 12.4, 6.38, 6.25, 6.19, 3.13, 3.6
Krankenhaus	12.2, 10.13, 10.12, 10.9, 3.6
Krankenkasse	10.15, 3.20
Krankenversicherung	10.15
Kredit	9.1
Kreditkartendaten.....	3.35, 3.8

Kundendaten	10.9, 10.9, 10.3, 3.37, 3.36, 3.26, 3.16, 3.15, 3.10, 3.8, 3.8, 3.4
Kündigung.....	7.20, 7.19, 7.8
Ladeneingang	6.50
Lageplan.....	6.68, 6.54, 6.42, 6.27, 6.18, 6.8
Landesärztekammer Thüringen.....	10.22, 10.2
Lastschriftverfahren	9.2, 3.44, 3.40
Lehrernamen	3.24
Leistungs- und Verhaltenskontrolle	7.18, 7.16, 7.15, 7.12, 7.11, 7.4, 7.1
Leistungskontrolle.....	7.22, 1
Leserservice	3.9
Lichtbild	12.13, 6.51
Linse.....	6.49, 6.6
Liquidation.....	3.42
Liquidator.....	3.42
Listendaten.....	3.26
Live-Beobachtung	6.38
Logistikunternehmen	7.22
Löschen.....	12.7, 10.21, 10.18, 10.13, 10.13, 9.3, 7.7, 3.40, 3.9, 3.7
Löschung	12.6, 12.5, 10.21, 10.18, 10.5, 9.1, 9.1, 8.2, 7.21, 7.21, 7.10, 7.7, 7.6, 7.5, 7.3, 6.71, 6.50, 6.41, 3.42, 3.41, 3.39, 3.7, 3.3
Löschungsfrist.....	10.2, 6.50
Makler	3.37
Markt- und Meinungsforschung.....	3.2
Mediengruppe	3.9
Medienprivileg	4.3
Mehrfamilienhaus	6.75, 6.31, 6.27, 6.26, 6.13, 3.45, 3.27
Meinungsfreiheit	12.5, 7.2
Meldeadresse.....	3.42
Meldeformular	6.37, 6.9
Meldepflicht	12.9, 6.70, 6.39, 6.33, 6.28, 6.21, 6.2, 6.1, 5.1, 4.1, 3.2, 1
Melderegister	6.39
Melderegisterpflicht	3.2
Meldeunterlagen.....	6.39
Meldung nach § 4d Abs. 1 BDSG.....	7.5, 6.9
Messdaten	3.31
Microsoft.....	12.14, 12.1
Mieter ...	6.75, 6.48, 6.47, 6.35, 6.31, 6.27, 6.26, 6.13, 6.5, 3.45, 3.27

Mieterselbstauskunft	3.12
Mietvermittlung	3.12
milderes Mittel	6.76, 6.71, 6.69, 6.59, 6.40, 6.4
Mitarbeiter 14, 12.5, 10.21, 10.17, 10.15, 10.11, 10.7, 10.5, 10, 10.2, 10.1, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.13, 7.11, 7.8, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 6.74, 6.71, 6.69, 6.65, 6.59, 6.44, 6.39, 6.32, 6.28, 6.10, 6.9, 6.8, 6.6, 5.1, 4.2, 4.1, 3.34, 3.25, 3.18, 3.10, 3.9, 3.8, 3.7, 3.6, 2.7, 2.3, 2.1, 1	
Mitarbeiterschutz	6.9
Mitarbeiterüberwachung	7.11, 6.8
Mitgliederdaten	4.2, 3.25, 3.18, 3.18
Mitgliederzeitschrift.....	4.3
Mitgliedsantrag	4.2, 3.18
Mitgliedsbeitrag	3.25, 3.18
Mithören.....	10.11, 10.10
Mitteilungsblatt	4.3
Monitor	7.3, 7.1, 6.74, 6.64, 6.60, 6.23, 6.18, 6.17, 6.13
Monitoring	7.12, 6.74, 6.65, 6.59, 6.58, 6.41, 6.40, 6.38, 6.18, 6.3
Mülltonne	6.5
multiresistente Keime	10.1
Nachbargrundstück	6.58, 6.52, 6.49, 6.44, 6.43, 6.37, 6.31, 6.21
Nachbarn 6.64, 6.52, 6.49, 6.48, 6.44, 6.34, 6.33, 6.24, 6.23, 6.22, 6.21, 6.18, 6.16, 6.13	
Nachbarparzelle	6.49
Nachbarschaft.....	6.21, 6.18, 6.14, 6.8, 6.7, 6.5
Nachweis 10.21, 10.4, 7.21, 6.69, 6.68, 6.62, 6.59, 6.53, 6.27, 6.20, 6.19, 6.18, 6.16, 6.7, 6.5, 3.14, 2.6	
Namen 10.21, 10.17, 10.16, 10.9, 10.3, 8.1, 6.31, 6.30, 6.29, 6.14, 6.12, 4.3, 3.46, 3.45, 3.43, 3.42, 3.40, 3.32, 3.27, 3.25, 3.24, 3.23, 3.21, 3.17, 3.14, 3.12, 3.10, 3.8, 3.6, 3.3, 3.2	
Namensnennung.....	3.10
nationales Recht	12.9, 2.1
Navigieren.....	3.33
Negativauskunft	9.3, 3.43
Netzwerkdurchsetzungsgesetz	12.5
Newsletter	3.40, 3.9
nicht-öffentlich zugänglicher Bereich.....	6.75, 6.64, 6.43, 6.41, 6.26
nicht-öffentlich zugänglicher Raum	7.17, 6.36, 6.28, 6.27, 6.18, 6.13
nicht-öffentliche Stellen 10.22, 10.10, 10.6, 10.5, 7.17, 7.12, 7.5, 6.70, 6.69, 6.65, 6.64, 6.59, 6.58, 6.39, 6.35, 6.26, 6.23, 6.21,	

6.18, 6.11, 6.9, 6.4, 6.3, 5.1, 3.35, 3.34, 3.29, 3.23, 3.18, 3.13, 3.12, 2.7, 2.4, 2.1	
NIS-Richtlinie	12.9
Notstand	10.1
Nutzungsrecht	6.53
Obergeschoss	6.50
Objekt.....	6.66, 6.54, 6.50, 6.47, 6.44, 6.36, 6.19, 6.8, 6.5, 2.7
Objektüberwachung	6.5
öffentlich zugängliche großflächigen Anlagen	6.61, 6.38
öffentlich zugänglicher Bereich 6.71, 6.69, 6.67, 6.65, 6.64, 6.59, 6.54, 6.51, 6.50, 6.48, 6.43, 6.41, 6.33, 6.21, 6.20, 6.17, 6.16, 6.15, 6.13, 6.11, 6.3, 2.6	
öffentlich zugänglicher Raum 7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.64, 6.61, 6.60, 6.59, 6.58, 6.55, 6.54, 6.53, 6.52, 6.50, 6.48, 6.43, 6.37, 6.36, 6.35, 6.34, 6.33, 6.31, 6.29, 6.27, 6.26, 6.24, 6.23, 6.22, 6.21, 6.20, 6, 6.16, 6.13, 6.11, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3	
öffentlich zugängliches Waldgebiet.....	6.70
öffentliche Stellen	10.5, 6.61, 6.57, 4.4, 4.1, 2.1
öffentliche Verkehrsmittel	6.72
öffentlicher Platz	6.6
öffentlicher Raum	6.61, 6.48, 6, 6.7, 3.34
öffentlicher Verkehrsraum	6.64, 6.44, 6.21, 6.17
Öffnungsklauseln	2.1
Onboard-Kamera.....	6.62
Onlinekauf.....	9.2
Onlineshop	3.35
Onlineunternehmen	9.2
Ordnungswidrigkeit 11.1, 6.63, 6.62, 6.32, 6.30, 5.1, 3.42, 3.31, 3.7, 1	
Ordnungswidrigkeitenverfahren	11.1, 6.62, 6.30, 2.2
Orientierungshilfe 10.13, 7.17, 7.12, 6.72, 6.65, 6.59, 6.41, 6.40, 6.37, 6.35, 6.26, 6.21, 6.9, 6.4, 6.3, 3.11	
Orientierungshilfe Videoüberwachung	6.27
Pächter.....	6.49, 6.29, 3.8
Parkkralle	3.6
Parzelle.....	6.49
Passwort	12.13, 12.11, 10.5, 7.13, 2.7
passwortgeschützter Bereich	3.24

Patient	10.22, 10.15, 10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 10.6, 10.4, 10.3, 10.2, 10.1, 3.26, 1
Patientenakte	351, 10.18, 10.11, 10.10, 10.7, 10.6, 3.26
Patientendaten	10.14, 10.11, 10.9, 10.6, 10.5, 10.4, 3.26
Patientenfoto	10.8
Personal.....	10.1, 7.1, 6.74, 6.71, 6.59, 6.38, 6.3, 3.10, 2.2
Personalausweis	12.13, 3.32, 3.22, 3.14, 3.12, 3.6
Personalausweisgesetz	12.13, 3.14, 3.12
Personalausweisregister	12.13
Personalausweisvorlage	3.22
Personaldienstleister.....	7.19, 7.8
personalisierte Werbung.....	12.12
personenbezogene Date.....	10.16
personenbezogene Daten	14, 12.10, 12.9, 12.7, 12.4, 12.3, 11.1, 10.22, 10.21, 10.20, 10.19, 10.18, 10.17, 10.15, 10.13, 10.12, 10.11, 10.10, 10.9, 10.8, 10.7, 10.5, 10.3, 10.1, 9.1, 8.2, 7.22, 7.21, 7.20, 7.18, 7.16, 7.15, 7.13, 7.10, 7.10, 7.8, 7.7, 7.6, 7.5, 7.4, 7.2, 7.1, 6.75, 6.72, 6.71, 6.69, 6.64, 6.59, 6.58, 6.56, 6.53, 6.52, 6.46, 6.45, 6.44, 6.43, 6.41, 6.39, 6.38, 6.37, 6.36, 6.34, 6.33, 6.32, 6.27, 6.26, 6.25, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.8, 6.7, 6.6, 6.4, 6.2, 5.1, 4.5, 4.4, 4.3, 4.2, 4.1, 3.47, 3.46, 3.45, 3.44, 3.41, 3.39, 3.38, 3.37, 3.36, 3, 3.32, 3.31, 3.30, 3.29, 3.28, 3.27, 3.26, 3.21, 3.20, 3.19, 3.18, 3.17, 3.16, 3.15, 3.14, 3.13, 3.11, 3.10, 3.9, 3.8, 3.7, 3.6, 3.5, 3.4, 3.3, 3.2, 2.7, 2.6, 2.5, 2.3, 2.2, 2.1, 1
Personengesellschaft	3.28, 2.5, 2.4
persönliche Daten	12.4, 10.16, 10.12, 6.48, 6.13, 3.45, 3.19, 3.6, 3.5, 2.2
Persönlichkeitsrecht	7.7, 7.1, 6.74, 6.71, 6.68, 6.66, 6.62, 6.56, 6.51, 6.48, 6.46, 6.34, 6.31, 6.23, 6.22, 6.20, 6.19, 6.18, 6.14, 6.13, 6.12, 3.46, 3.27, 2.6
Pflegedienst.....	10.5
Piktogramm.....	7.1, 6.60, 6.36, 6.8
Pkw	6.75, 6.72, 6.62, 6.36, 6.4, 3.12
Polizei	12.14, 12.13, 10.3, 6.62, 6.59, 6.46, 6.44, 6.30, 6.19, 6.5, 3.34, 3.2, 3.1
Positionsbestimmung	3.33
Postdienstunternehmen	3.20
Postgesetz.....	3.48
Postzustellung	4.4

Pranger	7.2
Presse	4.3, 3.34, 3.33, 3.21
Pressefreiheit	4.3, 3.21
Privacy Shield	12.6, 10.12
privater Hauseigentümer	6.37
Privatgrundstück	6.64, 6.33, 6.18, 6.17
Privatinsolvenz	9.1
Privatsphäre	12.4, 12.3, 10.1, 6.65, 6.23, 6.14, 6.13, 3.45
Privatweg	6.53
Probeabonnement	3.9
Produkte zur Pooldeinfektion	3.14
Pseudonym	3.27
Psychotherapeut	10.6
qualifizierte elektronische Signatur	3.38
Rabattcoupons	7.16
rechtliche Grundlage	3.45, 3.30, 3.9
Rechtsanwalt	10.6, 6.36, 6.30, 6.12, 3.23, 3.4, 2.4
Rechtsanwalts-Partnerschaft	2.4
Rechtsprechung	6.62, 6.58, 6.50, 6.48, 6.44, 6.21, 3.32, 1
Rechtsverstöße	6.54, 6.50, 6.44, 3.31
Register	6.32, 6.28
Registermeldung	6.32
Reihenhaussiedlung	6.14
rein redaktionelle oder journalistische Tätigkeit	3.21
Religionsausübung	3.48
Religionsgesellschaft	3.48
Reparaturen	6.5
Restaurant	7.1, 6.41, 6.6
Restschuldbefreiung	9.1
Rezept	10.19, 10.9, 10, 10.3
Router	12.11
Rückabwicklung	3.16
Rundfunk	3.20
Sachbeschädigung	6.75, 6.72, 6.59, 6.54, 6.50, 6.44, 6.27, 6.5, 6.3
Sachbeschädigungsdelikt	6.5
Sauna	6.69, 6.40, 6.37, 3.14
Schadenersatz	6.4, 3.4
Schaufenster	6.50, 6.23, 6.5, 3.33
Schornsteinfeger	3.36
Schredder	10.21, 10.13, 3.39, 3.29

Schriftform.....	10.7, 7.21, 7.19, 6.71, 6.2, 3.38, 3.37, 3.28, 2.5
Schufa	9.1, 3.20
Schule.....	12.1, 3.24
Schulhomepage	3.24
Schutz 12.9, 12.7, 12.3, 10.18, 10.12, 10.11, 10.8, 10.1, 7.17, 7.4, 6.74, 6.71, 6.66, 6.54, 6.54, 6.53, 6.50, 6.48, 6.44, 6.35, 6.34, 6.32, 6.21, 6.13, 6.10, 6.6, 4.1, 3.27, 2.6, 1	
Schutz der Patienten.....	10.8, 10.7
Schutz von Leben.....	6.72, 6.61, 6.38
Schutzmaßnahme	10.1, 7.3
schutzwürdige Interesse	6.65
schutzwürdige Interessen 10.3, 7.16, 7.5, 7.1, 6.75, 6.74, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.64, 6.62, 6.60, 6.58, 6.53, 6.50, 6.44, 6.41, 6.40, 6.38, 6.37, 6.36, 6.35, 6.29, 6.28, 6, 6.26, 6.23, 6.20, 6.18, 6.13, 6.11, 6.9, 6.8, 6.6, 6.4, 6.3, 4.3, 4.1, 3.45, 3.37, 3.31, 3.28, 3.26, 3.19, 3.15, 3.14, 3.8, 3.4, 3.3	
Schwärzen	6.71, 6.53
schwarzes Brett	3.25
Schweigepflicht.....	10.16, 10.14, 10.7, 10.6, 10.2, 7.9
Schweigepflichtentbindung.....	10.14, 10.1, 7.9
Schwimmbäder.....	6.40, 6.37, 6.32, 3.14
Screenshot	6.72, 6.68, 6.50, 6.8, 3.6
Selbstbedienungsladen	6.3
Seminararbeit	3.17
Seniorenheim	10.17
Server	12.15, 12.11, 10.19, 10.5, 6.50, 6.1
Sicherheitsstufe	10.21, 10.18, 10.13, 3.47, 3.39, 3.34, 3.29
Sicherheitstechnik	6.10
Sicherheits-Updates	12.14
Sichtbereich.....	6.49
Signaturgesetz	12.8, 3.38
Signaturverordnung.....	12.8
Skimming	3.35
smarte Lautsprecher	12.15
Smart-Home	6.10
Smartphone	12.15, 12.11, 12.4, 10.22, 10.5, 3.33, 3.24
Software	12.14, 12.12, 12.11, 12.10, 10.5, 6.51, 4.5, 3.35, 3.5, 2.7
Sorgerecht	10.16
soziale Netzwerke	14, 13.1, 12.5, 12.5, 12.4, 7.2
Spaziergänger.....	6.70, 6.25, 6.23, 6.11

Speicherdauer.....	7.5, 7.4, 6.36, 6.32, 6.8, 6.3
Speicherfrist.....	9.1, 6.71, 6.41, 6.36
Speicherkarte.....	6.66
Speicherung 12.13, 12.7, 10.21, 10.18, 10.13, 10.9, 10.7, 10.3, 9.3, 9.1, 8.2, 7.10, 7.6, 7.5, 6.72, 6.71, 6.64, 6.52, 6.50, 6.48, 6.41, 6.40, 6.34, 6.23, 6.18, 6.15, 6.13, 6.13, 6.8, 6.5, 6.4, 6.3, 4.2, 3.47, 3.44, 3.43, 3.34, 3.32, 3.14, 3.13, 3.12, 3.10, 3.9, 3.7, 3.2, 2.7	
Sperrung.....	12.5, 10.18, 7.10, 7.6
Spielhalle.....	6.71
Spielplatz.....	6.53
Spielzeug.....	12.15
Spindbereich	6.69, 6.40
Sportplatz	6.11
Sportverein.....	6.11, 4.2
Standardvertragsklauseln	10.12, 3.30
Stellplatz	6.4, 3.12
Steuerkanzlei.....	3.47
Steuerrecht	7.6, 3.32
Strafanzeige.....	10.6, 7.2, 6.75
Straftat 11.1, 10.3, 7.22, 7.16, 6.71, 6.69, 6.66, 6.40, 6.29, 6.27, 6.5, 6.4, 4.1, 3.34, 3.31, 3.22, 2.6	
Strafverfolgung	12.5, 10.6, 10.3, 6.72, 6.71, 6.66, 6.38, 5.1
Straße 6.76, 6.75, 6.67, 6.62, 6.61, 6.53, 6.50, 6.48, 6.37, 6.34, 6.33, 6.30, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.8, 6.5, 6.4, 3.45, 3.32	
Stundenabrechnungen	7.6
Tankstelle	6.9
Täter.....	11.1, 6.67, 6.62, 6.48, 6.20, 2.7
Tätigkeit 10.17, 10.4, 10.2, 7.22, 7.14, 7.3, 6.69, 6.66, 6.58, 6.57, 6.56, 6.54, 6.53, 6.52, 6.41, 6.37, 6.36, 6.30, 6.18, 6.16, 6.7, 5.1, 4.3, 3.48, 3.36, 3.34, 3.30, 3.21, 3.17, 3.16, 3.15, 2.7, 2.5, 2.3, 2.2, 2.1	
tatsächliche Anhaltspunkte.....	7.16, 5.1, 4.1
technisch-organisatorische Maßnahmen 12.14, 10.19, 10.18, 10.13, 10.10, 10.5, 9.3, 7.13, 6.41, 6.7, 4.5, 4.2, 3.41, 3.39, 3.38, 3.34, 3.29, 2.7	
technisch-organisatorische Maßnahmen	3.21
Telefonwerbung	8.1, 3.9
Telekommunikation	12.10, 12.2, 6.10, 3.20

Telekommunikationsgesetz	12.15, 12.9, 8.1
Telemediengesetz	12.9, 12.7
Theater	3.3
Therme	6.69
Thüringer Gesetz über betreute Wohnformen und Teilhabe	10.17
Thüringer Innenministerium	3.1
Thüringer Landesverwaltungsamt	10.22
Tonaufnahmen	6.32, 6.9
Tourenpläne	7.6
Tracking	12.12, 12.3
Türklingel	6.13
Türspion	6.13
Übermittlung 10.22, 10.19, 10.14, 10.11, 10.10, 10.3, 10.1, 6.5, 4.4, 4.3, 3.45, 3.41, 3.37, 3.35, 3.31, 3.30, 3.28, 3.26, 3.25, 3.18, 3.17, 3.4, 2.7, 2.1	
Überwachung 7.11, 7.5, 7.3, 7.2, 7.1, 6.75, 6.74, 6.72, 6.71, 6.69, 6.66, 6.64, 6.62, 6.61, 6.60, 6.59, 6.58, 6.55, 6.54, 6.52, 6.50, 6.48, 6.44, 6.40, 6.37, 6.36, 6.29, 6.28, 6.27, 6.26, 6.23, 6.21, 6.18, 6.15, 6.13, 6.10, 6.9, 6.8, 6.5, 6.1, 3.22, 2.6	
Überwachungsdruck 6.67, 6.56, 6.55, 6.48, 6.46, 6.34, 6.28, 6.20, 6.16, 6.13	
Umfrage	10.20, 6.40, 3.30, 3.28, 3.2
Umgang mit personenbezogenen Daten	3.41
Umkleidekabine	6.69, 6.40
Umtausch	3.10
unbefugtes Mitlesen	10.11
Unfallbeteiligte	6.62
Unfalldatenspeicher	6.62
Unternehmen 14, 13.2, 12.14, 12.13, 12.11, 12.9, 12.3, 10.21, 10.18, 10.12, 10.5, 10.3, 10.2, 9.3, 9.2, 8.2, 7.22, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.14, 7.12, 7.10, 7.9, 7.8, 7.7, 7.4, 7.2, 7.1, 6.72, 6.69, 6.65, 6.59, 6.47, 6.39, 6.38, 6.32, 6.28, 6.8, 6.3, 5.1, 4.5, 4.4, 4.3, 4.1, 3.47, 3.46, 3.44, 3.43, 3.42, 3.41, 3.37, 3.36, 3.35, 3.34, 3.32, 3.30, 3.26, 3.23, 3.21, 3.20, 3.19, 3.17, 3.15, 3.14, 3.13, 3.12, 3.11, 3.10, 3.8, 3.7, 3.6, 3.5, 3.4, 3.2, 2.6, 2.5, 2.3, 2.2, 2.1, 1	
Unternehmensdaten	3.46
Unternehmenskauf	3.26
Unternehmensverkauf	3.26
Unterschriften-Pad	3.38

Unterschriftensammlung.....	3.28
Untersuchung	12.9, 10.16, 10.14, 10.2, 7.9
Untersuchungsausschuss.....	3.1
unzulässige Datenerhebung.....	3.15
Unzuständigkeit	3.21, 3.20
Urkunde.....	10.22, 6.57, 2.5
Urkundenverifikation	10.22
USA	12.11, 10.19, 3.30
Vandalismus 7.17, 6.69, 6.67, 6.54, 6.53, 6.50, 6.48, 6.44, 6.27, 6.21, 6.20, 6.16, 6.13, 6.8, 6.7, 6.6, 6.5	
Veranstalter	3.3
verantwortliche Stelle 12.14, 11.1, 10.13, 10.11, 10.10, 10.5, 10.4, 9.3, 8.2, 7.13, 7.10, 7.8, 7.7, 7.6, 7.1, 6.76, 6.75, 6.72, 6.71, 6.70, 6.69, 6.65, 6.60, 6.57, 6.55, 6.47, 6.46, 6.45, 6.41, 6.39, 6.36, 6.27, 6.26, 6.23, 6.20, 6.18, 6.17, 6.11, 6.9, 6.8, 6.7, 6.4, 6.3, 6.2, 5.1, 4.3, 4.2, 3.45, 3.43, 3.42, 3.41, 3.40, 3.39, 3.38, 3.37, 3.34, 3.29, 3.28, 3.20, 3.19, 3.18, 3.15, 3.14, 3.13, 3.11, 3.8, 3.7, 3.4, 2.5, 2.4, 2.3, 2.2	
Verarbeitung 13.2, 12.7, 12.4, 12.3, 10.21, 10.18, 10.17, 10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 10.3, 10.1, 9.2, 9.1, 7.22, 7.18, 7.17, 7.16, 7.5, 7.4, 6.75, 6.72, 6.71, 6.69, 6.64, 6.52, 6.46, 6.41, 6.39, 6.36, 6.28, 6.27, 6.26, 6.23, 6.20, 6.18, 6.16, 6.12, 6.8, 6.7, 6.6, 6.4, 4.3, 4.2, 4.1, 3.47, 3.45, 3.44, 3.41, 3.40, 3.39, 3.38, 3.36, 3.34, 3.32, 3.31, 3.30, 3.28, 3.26, 3.25, 3.22, 3.20, 3.19, 3.18, 3.17, 3.16, 3.15, 3.14, 3.10, 3.8, 3.5, 3.4, 3.2, 2.7, 2.6, 2.5, 2.4, 2.3, 2.2, 2.1	
Verband.....	4.3, 3.18
Verbreiten	7.14, 6.62
Verein 6.11, 4.3, 4.2, 3.41, 3.40, 3.40, 3.39, 3.28, 3.25, 3.25, 3.18, 3.18	
Verfahrensregister	6.2
Verfassungsschutz.....	12.13
Verfolgung	11.1, 10.3, 6.62, 6.30, 6.6, 3.44, 3.31, 3.21, 3.18, 3.4
Verfolgungsbehörde.....	6.62
Verkehrsgeschehen	6.62
Verkehrsraum.....	6.64, 6.62, 6.48, 6.18, 6.17, 6.15, 6.13
Verkehrsunfall.....	10.3, 6.62
Verletzung.....	10.16, 10.6, 6.51, 6.46, 6.16, 6.6, 3.34, 3.21
Verletzungsgefahr	7.12
Vermieter	10.10, 6.47, 6.35, 6.31, 6.27, 6.26, 6.13, 3.45, 3.12

vernetztes Fahren	12.4
Veröffentlichung 10.12, 9.1, 7.21, 7.14, 7.2, 5.1, 4.3, 3.40, 3.25, 3.24, 3.21, 3.17	
Verschlüsselung	10.22, 10.19, 10.5, 2.7
Versichertendaten	10.15
Versicherung	10.6, 7.16, 7.3, 6.5, 3.37, 3.15
Versicherungsmakler	3.37, 3.37, 3.16
Verstorbene	10.4, 3.13
Vertrag 12.6, 10.18, 10.5, 7.22, 7.9, 7.8, 6.27, 3.47, 3.40, 3.39, 3.38, 3.37, 3.34, 3.16, 3.5	
Vertrauensdienstegesetz	12.8
Vertretungsplan	3.24
Verwertbarkeit	6.62
Verwertung	6.72, 6.62
Video	12.5, 12.4, 6.68, 6.62, 6.52, 6.50, 6.32
Videobeobachtung	7.1, 6.64, 6.23, 6.13, 6.7
Videokamera 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.67, 6.64, 6.62, 6.60, 6.58, 6.57, 6.55, 6.53, 6.52, 6.50, 6.48, 6.46, 6.45, 6.44, 6.41, 6.40, 6.36, 6.31, 6.30, 6.28, 6.24, 6.23, 6.22, 6.21, 6.20, 6.19, 6.16, 6.15, 6.14, 6.11, 6.10, 6.7, 6.6, 6.4, 1	
Videoüberwachung 14, 7.17, 7.12, 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.69, 6.66, 6.65, 6.64, 6.62, 6.61, 6.60, 6.59, 6.58, 6.57, 6.56, 6.55, 6.54, 6.53, 6.52, 6.50, 6.48, 6.47, 6.46, 6.45, 6.44, 6.42, 6.41, 6.39, 6.38, 6.37, 6.36, 6.35, 6.34, 6.33, 6.32, 6.31, 6.30, 6.29, 6.28, 6.28, 6.27, 6.26, 6.24, 6.23, 6.22, 6.21, 6.20, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.10, 6.10, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2, 6.1	
Videoüberwachung im Schwimmbad/Erlebnisbad	6.40
Videoüberwachungsanlage 7.3, 6.76, 6.71, 6.69, 6.68, 6.67, 6.65, 6.63, 6.60, 6.59, 6.53, 6.52, 6.51, 6.50, 6.49, 6.48, 6.45, 6.44, 6.43, 6.42, 6.41, 6.40, 6.38, 6.37, 6.36, 6.33, 6.31, 6.30, 6.29, 6.28, 6.27, 6.24, 6.23, 6.21, 6.20, 6.16, 6.13, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2, 6.1	
Videoüberwachungsverbesserungsgesetz	6.72, 6.38
Vogelhaus	6.23
VoIP	12.10, 12.3
Volkszählungsgesetz	6.48
Vorabkontrolle	7.12, 7.5, 6.9, 6.3
Vorgesetzter	7.18, 7.15, 7.13, 7.8, 6.28, 4.1, 3.6

Vorkommnis	6.76, 6.75, 6.72, 6.65, 6.59, 6.53, 6.50, 6.48, 6.33, 6.32, 6.27, 6.20, 6.16, 6.4, 6.3
Vor-Ort-Kontrolle	10.11, 10.4, 7.3, 6.43, 6.32, 6.12, 6.6, 3.47, 3.44, 3.2
Wahrnehmung	7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.57, 6.54, 6.53, 6.50, 6.48, 6.44, 6.40, 6.37, 6.36, 6.35, 6.34, 6.31, 6.29, 6.24, 6.23, 6.20, 6.18, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 3.4, 2.5, 2.3
Wahrung berechtigter Interessen	7.5, 7.4, 6.75, 6.64, 6.44, 6.36, 6.28, 6.26, 6.11, 6.4, 4.3, 3.45, 3.31, 3.28, 3.19, 3.15, 3.14, 3.4
Waldrand	6.63
Wanderweg	6.25
WannaCry	12.14
Wanzen	3.35
Warnschild	6.62
Wartebereich	10.11, 10.10, 6.8, 6.4
Wearables	10.20
Weg	12.12, 10.3, 7.22, 6.63, 6.63, 6.53, 6.53, 6.19, 6.11, 6.8, 6.8, 3.37, 3.18, 1
Wegerecht	6.53
Weihnachtsmann	3.48
Weihnachtspostamt	3.48
Weitergabe	12.4, 10.17, 10.16, 10.1, 7.19, 7.10, 6.48, 6.13, 3.45, 3.37, 3.31, 3.26, 3.8
Werbeemails	8.2
Werbung	12.12, 8.2, 3.40, 3.36, 3.26, 3.15, 3.9
Werkstätte	12.4, 7.14
WhatsApp	10.19
Widerruf	10.9, 3.16, 2.5
Widerspruch	12.6, 10.2, 3.37, 3.9, 3.8, 2.3, 2.2
Wildkamera	6.70, 6.58, 6.27, 6.2
Wildtierkamera	6.70, 6.2
Windows 10	12.1
Windows 8	12.14
Windows Server 2003	12.14
Windows XP	12.14
Windschutzscheibe	6.62
Wohnungstür	6.13
Zahlartensteuerung	3.19
Zahlmethode	3.19

Zahnarzt	10.15, 10.11
Zahnarztpraxis	10.15, 10.10
Zaun	6.49, 6.21, 2.7
Zeitung	4.3, 3.21, 3.9
Zentrale	7.16, 2.6
Zeugnisverweigerungsrecht	10.3, 6.30
zivilrechtliche Ansprüche	6.46
Zoomfunktion	6.50, 6.28, 6.23
Zugangskontrolle	7.13, 6.41, 2.7
Zugriffskontrolle	7.13, 3.34, 2.7
Zulassungskopie	3.6
zuständige Aufsichtsbehörde 12.6, 7.3, 6.68, 6.42, 6.37, 6.27, 6.20, 6.18, 6.14, 6.12, 6.2, 5.1, 4.3, 3.35, 3.21, 3.18	
Zuständigkeit 12.4, 11.1, 10.16, 10.15, 9.1, 7.16, 7.10, 6.68, 6.47, 6.23, 6.3, 3.48, 3.33, 3.23, 3.21, 3.20	
Zuverlässigkeit	13.2, 7.5, 2.5, 2.4, 2.3, 2.2
Zuwegung	6.53
Zwangsgeld	6.42, 6.17
Zweckbestimmung	6.62, 4.3, 3.40, 3.18
Zwecke 13.1, 12.7, 12.4, 10.21, 10.20, 10.18, 10.17, 10.16, 10.14, 10.13, 10.9, 10.8, 10.6, 10.3, 10.2, 9.3, 8.2, 7.22, 7.21, 7.20, 7.18, 7.17, 7.15, 7.11, 7.10, 7.8, 7.7, 7.6, 7.5, 7.4, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.56, 6.54, 6.53, 6.50, 6.48, 6.44, 6.43, 6.41, 6.40, 6.39, 6.38, 6.37, 6.36, 6.36, 6.35, 6.34, 6.33, 6.32, 6.32, 6.31, 6.30, 6.29, 6.28, 6.27, 6.25, 6.24, 6.23, 6.20, 6.18, 6.17, 6.16, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 4.3, 4.1, 3.47, 3.46, 3.45, 3.43, 3.40, 3.38, 3.37, 3.31, 3.28, 3.26, 3.22, 3.21, 3.18, 3.15, 3.14, 3.13, 3.7, 3.6, 3.4, 3.3, 3.2, 2.6, 2.1, 1	
zweckfremde Übermittlung	3.31

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)
Häblerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361/57 3112900, Telefax: 0361/57 3112904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: ReproPartner GbR
Liebknechtstr. 18
99085 Erfurt
Telefon: 0361/7891270
E-Mail: info@repropartner.de

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

Redaktionsschluss: 31. Januar 201:

Bildnachweis: TLfDI